NORTEL NETWORKS

Enterprise Edge Programming Operations Guide

Contents

Contents iii

Chapter 1 About this document 11

What's new in this document 11
How this guide is organized 11
Related documents 12
Regulations 13
- Safety 13
- Radio-frequency interference 14
- Telecommunication registration 14
- Hearing-aid compatibility 15
- Electromagnetic compatibility 15
- Telephone company registration 15
- Use of a music source 16
- Rights of the telecommunications company 16
- Repairs 16
- Safety 16
- Radio-frequency interference 17

Software licensing 18

Chapter 2 Enterprise Edge Overview 21

Hardware components 21
Software components 22
- Enterprise Edge Integrated Solution 22
- Enterprise Edge Voice Messaging 23
- Enterprise Edge Call Center 24
- Enterprise Edge Call Center Reporting 24
- Enterprise Edge Voice over IP gateway 24
- Enterprise Edge Unified Messaging 25
- Enterprise Edge TSP Server 25
- Enterprise Edge Personal Call Manager 25
- Enterprise Edge Call Detail Recording 25
- Nortel Networks Voice Service 25

Unified Manager 26
- Browser requirements 26
- Understanding the Unified Manager 27
- Menu descriptions 29
- Enterprise Edge system access 30

Chapter 3 Using Enterprise Edge Services 33

Routing and IP services supported by Enterprise Edge 33

IP Routing 34
IP Routing Overview 34
Enterprise Edge IP routing specifics 35
IP Addressing Overview 35
Static Routing 36
Routing Information Protocol (RIP) 36
Enabling RIP on Network Interfaces 36
Packet Filtering 36
LAN-to-LAN Fast Path Routing 37
Dynamic Host Configuration Protocol (DHCP) 37
Automatic Configuration using a DHCP server 38
Guidelines for Using DHCP 38
Domain Name Service (DNS) 39
Guidelines for Using DNS 39
Web Caching/Proxy 40
Guidelines for Using Web Caching/Proxy 40
Simple Network Management Protocol (SNMP) 41
Guidelines for Using SNMP 41
Quality of Service 42
QoS overview 42
DiffServ Networks 43
Legacy Networks 43
Admission Control 44
Packet Marking for DiffServ Networks 45
Port Range Setting for Legacy Networks 47
Relationship between the QoS Module and the VoIP QoS Monitor 48
Enterprise Edge QoS Restrictions and Defaults 48
LAN Connections 49
WAN Connections 49
WAN overview 49
Permanent WAN Connections 50
Backup Up WAN Connection 51
Backup WAN Links 52

Chapter 4 Setting up your Enterprise Edge system 53

Enterprise Edge required parameters 53
Setting up an Enterprise Edge IP Address 54
Setting up web-based administration 55
Browser settings 55
Logging on to Enterprise Edge 56
Logging off Enterprise Edge 57
Rebooting the Enterprise Edge server 57
Configuring system settings 57
System name 58
System name, date and time 61

Chapter 5 Configuring networking resources 63

Viewing Enterprise Edge resources 63
Configuring LAN settings 64
Configuring WAN settings 66
- WAN Primary Link Summary Parameters 67
- WAN Primary Link Line Parameters 68
- WAN Primary Link Frame Relay Parameters 70
- WAN Primary Link PPP parameters 73
- WAN Primary Link performance graphs and tables 73
- WAN Backup Links 73
- WAN Backup Summary Parameters 74
- WAN Backup Link Parameters 74
- WAN Backup Access Parameters 76

Chapter 6 Configuring Telephony Resources 77

Programming order 78
Terminals &Sets 80
- Copying settings from one telephone set to another 80
- Line access 81
- Capabilities 86
- Name 89
- User preferences 90
- Restrictions 91
- Telco features 92

Lines 95
- Copying settings from one line to another 95
- Trunk/Line data 96
- Restrictions 106
- Telco features 107

Restriction filters 108
Services 111
- Ringing service 112
- Restriction service 114
- Routing service 114
- Destination codes 117
- Setting up a route for local calling 119
- Setting up a route for long distance calling 120
- Adding a long distance carrier access code 121
- Programming for least cost routing 122
- Using dialing restrictions with routing 123
- Using a dialing plan to route outgoing PRI calls 123
- Common settings 126

System speed dial 128
Adding or changing a system speed dial 128
Passwords 130

COS passwords 130
Call log passwords 132
Registration password 132
Hospitality passwords 132
Time and date 134
General settings 135
Business name 136
Feature settings 136
Call log space 142
Direct dial 142
CAP assignment 143
Access codes 143
Remote access 146
DN lengths 148
Network Name Display 149
Programming Network Name Display 150
Call by Call service selection for PRI 151
Programming Call by Call service selection 154
Hospitality 155
Hunt groups 159
Adding or removing members from a group 160
Moving members of a group 161
Assigning or unassigning lines to a group 162
Setting the distribution mode 163
Setting the hunt delay 163
Programming busy line setting 164
Programming the queue time-out 164
Programming the overflow set 164
Setting the name 165
Companion 166
Registration 166
Changing the Registration password 167
Radio data 168
Register individual portables 170
System programming 170
Directed Call Pickup 171
Group Pickup 171
Wireless Call Forward No Answer 171
Telco features 172
Voice Message center numbers 172
Outgoing Name and Number Blocking 172
Software keys 173
System Identification Number 173
Entering the software keys 173
Hardware 175
Module 175

Card 176
T1 Parameters 181

Chapter 7 Configuring Enterprise Edge Services 185

Viewing Enterprise Edge services 186
DHCP 186
DHCP LAN settings 187
DNS settings 192
Routing 192
LAN Routing 193
WAN Routing 201
SNMP 202
SNMP Community List, Manager List, and Trap Community List 203
QoS 206
QoS performance graphs and tables 209
QoS filters 209
QoS Port Ranges 211
VoIP Gateway 212
VoIP local and remote gateways 212
QoS monitor 215
QoS Monitor Mean Opinion Score 216
Web cache 216
Net Link Manager 217
Call Detail Recording 218
Report parameters 219
Report options 220
Market parameters 221
PreFix Bins 222
Access Bin Settings 223
TAPI Service Provider 223
Console Service 224
Server Configuration 225
General Information 225
Diagnostic Logging 226
Alarm Service 226
Voice Mail 227

Chapter 8 Configuring Management Settings 229

User Manager 229
Alarm Manager 231

Chapter 9 Maintenance 233

System startup 233

Warm reset 234
Backup and restore 234
Backup, restore, upgrade utility (BRU) for Enterprise Edge system 234
Backup and restore telephony programming 237
Enterprise Edge system diagnostics and utilities 241
Saving System Settings 241
Downloading System Settings 241
Graphs and tables 243
Error Messages 244
MIB II Information 249
Maintenance programming for telephony resources 253
System version 253
Module/port status 254
System test log 257
System administration log 258
Network event log 260
Alarm codes 261
Event messages 261
Provisioning 271
Tests 272
CSU statistics 274
Link Status 278
Metrics 279
Moving telephones 279

Chapter 10 Troubleshooting your Enterprise Edge system 281

General troubleshooting information 281
Getting ready 281
Types of problems 282
Basic troubleshooting procedure 282
Viewing system performance and fault alarms 283
System performance graphs and tables 283
System Fault Alarm Banner 284
Problems with telephones 284
Problems with lines 285
Calls cannot be made (but can be received) 285
Dial tone absent on external lines 286
Hung lines at a telephone 286
Auto-answer line rings at a telephone 288
Prime telephone gets misdialed calls 289
Selected lines reads “Not in service” or “Not available” 290
Selected line pool shows “No free lines” 290
Problems with optional equipment 291
Problems with the Enterprise Edge ATA 2 291
Problems with the auxiliary ringer 292
Problems with external paging 292

Problems with Music on Hold and Background Music 293
Problems with module service 293
Digital Trunk Computer Module trouble 294
Monitoring the T1 or PRI signal 295
Problems with Trunk or Station Modules 295
Problems for network or remote users 296
Remote feature code gets no response 297
Dialed number gets ringback and the wrong person 297
Dialed number gets dial tone instead of ringback 297
Dialed number gets busy tone 298
Dialed number does not get through 298
Dialed feature code gets overflow tone 299
Dialed feature code gets busy tone 300
Line pool access code gets overflow tone 300
Line pool access code gets ringback 301
Line pool access code gets busy tone 301
Dialed number gets no response 301
Problems with Companion sets 302

Appendix A: Network Examples 303

Enterprise Edge in a network 303
The big picture 303
Networking Enterprise Edge with Meridian M1 over PRI 304
Benefits 304
Lines 304
PRI lines 305
T1 lines (Loop, E&M, DID, Ground start) 305
Target lines 305
Remote system access 306
Remote access on loop start trunks 306
Remote access on a private network 307
Remote access on T1 Direct Inward Dial (DID) trunks 307
Remote access on PRI trunks 307
Security 308
Class of Service 308
Restriction filters 308
Direct inward system access (DISA) 310
Coordinated dialing plan 310
Coordinated dialing plan using public lines 310
Destination code numbering in a network 311
Dialing plan using T1 E&M lines 312
Dialing plans with shared line pools 315
PRI Networking with Meridian 1 316
Additional Configuration 319
Meridian M1 Configuration 319

Call-by-Call Services Example 319
Enterprise Edge VoIP Gateway and M1 networking 322
Toll bypass with Enterprise Edge VoIP Gateway 325
Other networking examples 330
Public network 331
Call one or more Enterprise Edge telephones 331
Call Enterprise Edge and select tie lines to a private network 331
Call Enterprise Edge and select lines to the public network 332
Private network 333
Call one or more Enterprise Edge telephones 333
Call Enterprise Edge and select tie lines to other nodes in the private network 334
Call Enterprise Edge and select lines to the public network 335
Select T1 E&M trunks to the private network 336
Enterprise Edge Line Redirection feature 336
PRI dialing plan example for 2-way DID 338
PRI DID and 2-way DID 338

Appendix B: ISDN Overview 339

Welcome to ISDN 339
Analog versus ISDN 339
ISDN PRI channels 340
ISDN layers 340
ISDN Bearer capability 341
Services and features for ISDN PRI 341
ISDN hardware 344
Clock Source for ISDN 344
ISDN standards compatibility 345
Ordering ISDN PRI service in Canada 345
Ordering ISDN PRI service in United States 345
Supported ISDN protocols 345
ISDN programming 345
Program ISDN equipment 347

Appendix C: Setting Up Remote Routers 349

Creating an Outbound Traffic Filter 349
Sample Criteria, Ranges, and Actions for UDP Filtering 350

Glossary 351

Index 391

About this document 1

This guide explains how to program your Enterprise Edge system. For more information on the Enterprise Edge document suite, refer to Related documents on page 12.

Note: The Enterprise Edge system regulatory information is summarized in Regulations on page 13.

Software licensing information is contained in Software licensing on page 18.

What's new in this document

This release includes the following additional information:

- Data programming information previously contained in the Enterprise Edge Networking Operations Guide
- Hospitality programming

How this guide is organized

This document contains the following sections:

- Enterprise Edge Overview on page 21 provides an overview of the hardware and software components of the Enterprise Edge system as well as a description of the Unified Manager.
- Using Enterprise Edge Services on page 33 describes the services that can be used on the Enterprise Edge system.
- Setting up your Enterprise Edge system on page 53 includes information on how to set up your IP address and web-based administration, how to configure your system settings and other basic procedures such as logging on and off your Enterprise Edge system.
- Configuring Telephony Resources on page 77 describes the procedures used to program your Enterprise Edge system.
- Configuring networking resources on page 63 describes the procedures used to program the networking resources for your Enterprise Edge system.
- Configuring Enterprise Edge Services on page 185 describes the procedures used to program all the Enterprise Edge services.
- Configuring Management Settings on page 229 includes procedures used to program the system security including userids, passwords and profiles.
- Maintenance on page 233 includes all the maintenance procedures required to keep your system operational. It includes descriptions of how to perform both a

system and telephony programming backup and restore.

- Troubleshooting your Enterprise Edge system on page 281 allows you to solve problems in the Enterprise Edge system that require changes to system programming.
- Appendix A: Network Examples on page 303 includes some networking examples using the Enterprise Edge system.
- Appendix B: ISDN Overview on page 339 includes some background information about ISDN.
- Appendix C: Setting Up Remote Routers on page 349 explains how to set up a Nortel Networks (BayRS) router.
- Glossary on page 351 contains a list of Enterprise Edge terms and definitions.

Related documents

In addition to the *Enterprise Edge Programming Operations Guide*, the Enterprise Edge documentation suite contains the following documents.

- *Enterprise Edge Feature Programming Telephone Guide*
- *Enterprise Edge Installation and Maintenance Guide*
- *Enterprise Edge IP Telephony Configuration Guide*
- *Enterprise Edge Voice Messaging Set Up and Operation Guide*
- *Enterprise Edge Voice Messaging Reference Guide*
- *Enterprise Edge Voice Messaging Quick Reference Guide*
- *Enterprise Edge Voice Messaging Programming Record*
- *Enterprise Edge Voice Messaging AMIS Set Up and Operation Guide*
- *Enterprise Edge Voice Messaging AMIS User Guide*
- *Enterprise Edge Unified Messaging Client Installation Guide*
- *Enterprise Edge Unified Messaging Quick Reference Guide*
- *Enterprise Edge Software Keycode Installation Guide*
- *Enterprise Edge Call Center Set Up and Operation Guide*
- *Enterprise Edge Call Center Agent Cards*
- *Enterprise Edge Call Center Reporting Set Up and Operation Guide*
- *Enterprise Edge TSP Server Configuration Guide*
- *Enterprise Edge Personal Call Manager User Guide*
- *Enterprise Edge Attendant Console Set Up and Operation Guide*
- *Enterprise Edge Attendant Console User Guide*
- *Enterprise Edge Call Detail Recording System Administrator Manual*

- *Enterprise Edge ATA 2 Installation Guide*
- *Enterprise Edge ATA 2 User Guide*
- *Enterprise Edge Networking Set Up and Operation Guide*
- *Enterprise Edge Networking User Guide*

In addition, you can access the following telephone quick reference cards:

- *Enterprise Edge M7100 User Card*
- *Enterprise Edge M7208 User Card*
- *Enterprise Edge M7310 User Card*
- *Enterprise Edge M7324 User Card*
- *Enterprise Edge M7410 User Card*
- *Enterprise Edge CAP User Card*
- *Enterprise Edge Prime Telephone User Card*
- *Enterprise Edge Telephone Feature Card*

Regulations

Safety

Enterprise Edge equipment meets all applicable requirements of both the CSA C22.2 No. 950-95 and UL-1950 Edition 3.

Risk of shock.
Ensure the computer is unplugged from the power socket and that any telephone or network cables are unplugged before opening the computer.

Read and follow installation instructions carefully

Only qualified persons should service the system.

The installation and service of this hardware is to be performed only by service personnel having appropriate training and experience necessary to be aware of hazards to which they are exposed in performing a task and of measures to minimize the danger to themselves or other persons.

Electrical shock hazards from the telecommunication network and AC mains are possible with this equipment. To minimize risk to service personnel and users, the Enterprise Edge system must be connected to an outlet with a third-wire ground.

Service personnel must be alert to the possibility of high leakage currents becoming available on metal system surfaces during power line fault events near network lines. These leakage currents normally safely flow to Protective Earth ground via the power cord. Therefore, it is mandatory that connection to an earthed outlet is performed first and removed last when cabling to the unit. Specifically, operations requiring the unit to be powered down must have the network connections (central office lines) removed first.

Radio-frequency interference

Equipment generates RF energy.

This equipment generates, uses, and can radiate radio-frequency energy. If not installed and used in accordance with the installation manual, it may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Part 15 of the FCC Rules and with ICES.003, CLASS A Canadian EMI Requirements. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his or her own expense, will be required to take whatever measures may be required to correct the interference.

Telecommunication registration

Enterprise Edge equipment meets all applicable requirements of both Industry Canada CS-03 and US Federal Commission FCC Part 68 and has been registered under files Industry Canada 332-5980 A and FCC AB6CAN-20705-KF-E (key system), AB6CAN-20706-MF-E (hybrid system), and AB6CAN-23740-PF-E (PBX system). Connection of the Enterprise Edge telephone system to the nationwide telecommunications network is made through a standard network interface jack that you can order from your local telecommunications company. This type of customer-provided equipment cannot be used on party lines or coin lines.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment. Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician.

Hearing-aid compatibility

Enterprise Edge telephones are hearing-aid compatible, as defined in Section 68.316 of Part 68 FCC Rules.

Electromagnetic compatibility

Enterprise Edge equipment meets all FCC Part 15, Class A radiated and conducted emissions requirements.

Enterprise Edge does not exceed the Class A limits for radiated and conducted emissions from digital apparatus as set out in the Radio Interference Regulations of Industry Canada.

Telephone company registration

It is usually not necessary to call the telecommunications company with information on the equipment before connecting the Enterprise Edge system to the telephone network. If the telecommunications company requires this information, provide the following:

- telephone number(s) to which the system will be connected
- FCC registration number (on label affixed to Enterprise Edge)
- universal service order code (USOC)
- service order code (SOC)
- facility interface code (FIC)

Use of a music source

In accordance with U.S. Copyright Law, a license may be required from the American Society of Composers, Authors and Publishers, or similar organization if Radio or TV broadcasts are transmitted through the Music On Hold or Background Music features of this telecommunication system.

Nortel Networks hereby disclaims any liability arising out of the failure to obtain such a license.

Rights of the telecommunications company

If the Enterprise Edge system is causing harm to the telephone network, the telecommunications company may discontinue service temporarily. If possible, the telecommunications company will notify you in advance. If advance notice is not practical, the user will be notified as soon as possible. The user will be given the opportunity to correct the situation and informed of the right to file a complaint to the FCC.

The telecommunications company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of the system. If this happens, the telecommunications company will give you advance notice in order for you to make any necessary modifications to maintain uninterrupted service.

Repairs

In the event of equipment malfunction, all repairs to certified equipment will be performed by an authorized supplier.

Safety

WARNING

The instructions in this manual are intended to be performed by Qualified Service Personnel.

CE

The CE mark indicates that the Enterprise Edge equipment meets the requirements of the following EU Directives:

- Low Voltage Directive (73/23IIC)
- Electromagnetic Directive (89/336/EEC)

Risk of shock.

Ensure the computer is unplugged from the power socket and that any telephone or network cables are unplugged before opening the computer.

Read and follow installation instructions carefully

Only qualified persons should service the system.

The installation and service of this hardware is to be performed only by service personnel having appropriate training and experience necessary to be aware of hazards to which they are exposed in performing a task and of measures to minimize the danger to themselves or other persons.

Electrical shock hazards from the telecommunication network and AC mains are possible with this equipment. To minimize risk to service personnel and users, the Enterprise Edge system must be connected to an outlet with a third-wire Earth.

Service personnel must be alert to the possibility of high leakage currents becoming available on metal system surfaces during power line fault events near network lines. These leakage currents normally safely flow to Protective Earth via the power cord. Therefore, it is mandatory that connection to an earthed outlet is performed first and removed last when cabling to the unit. Specifically, operations requiring the unit to be powered down must have the network connections (exchange lines) removed first.

Radio-frequency interference

This is a Class A product. In a domestic environment this product may cause interference. The user may be required to take adequate measures.

Read and follow installation instructions carefully

This product uses Telecommunication Network Voltage (TNV) circuits which include the following ports: analogue lines (including PFT), modems, ATA, BRI, AC15A and TCM Isolator.

This product uses Safety Extra Low Voltage (SELV) circuits which include the following ports: TCM extensions, external music source (MSCX), auxiliary ringer (AUX), paging system relay (PAGE), LAN interface, WAN interface and the serial port.

Software licensing

Copyright (c) 1995-1999 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/)."

4. The names "Apache Server" and "Apache Group" must not be used to endorse or promote products derived from this software without prior written permission.

For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache" nor may "Apache" appear in their names without prior written permission of the Apache Group.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/)."

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE GROUP OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Group and was originally based on public domain software written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign. For more information on the Apache Group and the Apache HTTP server project, please see <http://www.apache.org/>

Enterprise Edge Overview 2

The Enterprise Edge system consists of software and hardware components that offer traditional telephony technology, basic voice messaging and IP telephony.

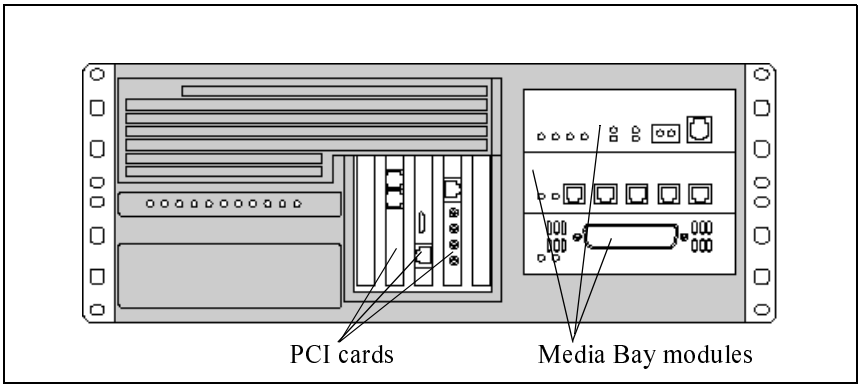
The system components are summarized in:

- Hardware components on page 21
- Software components on page 22

A Unified Manager is used to provide access to all Operations and Maintenance programming on the Enterprise Edge system. For more information on the Unified Manager, refer to Unified Manager on page 26.

Hardware components

The Enterprise Edge system consists of PCI cards and a number of Media Bay modules installed in a PC server.



The main hardware components of the Enterprise Edge system include:

- PCI standard cards which perform call processing as well as media processing of the voice channels. The following types of cards may be included:

  - Media Services Card (MSC)

  - V.90 Interface

  - LAN interface Card (10/100 Base T Ethernet NIC)

  - WAN Interface Card with CSU/DSU

- Station set media Bay modules which provide access to telephone lines. The Enterprise Edge system includes the following station set media bay modules:

  - 16-port Digital Station Media Bay Module (EE-DSM 16) which allows the connection of 16 digital telephone sets to the system

  - 32-port Digital Station Media Bay Module (EE-DSM 32) which allows the connection of 32 digital telephone sets to the system

- Analog Station Media Bay Module (EE-ASM 8) which allows the connection of analog station sets to the system

- Trunk media bay modules which provide access to telecommunications trunks. The Enterprise Edge system includes the following trunk media bay modules:

  - Digital Trunk Media Bay Module (EE-DTM) which provides the connection between a standard digital PSTN T1 or PRI line and the Enterprise Edge system.

  - Caller ID Trunk Media Bay Module (EE-CTM) which provides the ability to access four analog Caller ID PSTN lines.

- Station sets and adapters

For a detailed description of each of the hardware components, refer to the *Enterprise Edge Installation and Maintenance Manual*.

Software components

The Enterprise Edge system provides a number of software applications, assembled into software packages that are enabled using software key codes. A software keycode is a password number provided to the installer. The available Enterprise Edge software applications are:

- Enterprise Edge Integrated Solution on page 22
- Enterprise Edge Voice Messaging on page 23
- Enterprise Edge Voice over IP gateway on page 24
- Enterprise Edge Unified Messaging on page 25
- Enterprise Edge Call Center on page 24
- Enterprise Edge Call Center Reporting on page 24
- Enterprise Edge TSP Server on page 25
- Enterprise Edge Personal Call Manager on page 25
- Enterprise Edge Call Detail Recording on page 25
- Nortel Networks Voice Service on page 25

For more information on the software application packaging, refer to *Enterprise Edge Installation and Maintenance Manual* and *Enterprise Edge Software Keycode Installation Guide*.

Enterprise Edge Integrated Solution

Enterprise Edge Integrated Solution software supplies standard telephony, voice messaging and integrated QoS routing functionality plus the following additional features:

- Enterprise Edge Companion Wireless on page 23
- Enterprise Edge Unified Manager on page 23

Enterprise Edge Companion Wireless

The Enterprise Edge Companion Wireless software provides wireless functionality without losing the benefits of the wireline system.The system can be programmed so that users can publish one telephone number and receive all calls on both their desk set and their portable, allowing them to answer whichever is most convenient.

Enterprise Edge Unified Manager

The Enterprise Edge Unified Manager software provides programming, administration and maintenance. Enterprise Edge Unified Manager provides a series of windows and menus which allow you to navigate through the different areas of the application and program the system. For more information on the Unified Manager, refer to Unified Manager on page 26.

Enterprise Edge Voice Messaging

Enterprise Edge Voice Messaging is a Windows™ based application that allows the user to set up and administer the following Voice Messaging features:

- Voice messaging on page 23
- Auto attendant on page 23
- Custom Call Routing (CCR) on page 23
- Audio Messaging Interchange Specification (AMIS) Networking on page 24
- Enterprise Edge Networking on page 24

Voice messaging

Voice messaging records caller's messages and stores them in a mailbox for easy retrieval. Each Enterprise Edge telephone in your system can have its own mailbox as well as personal greeting.

Auto attendant

Auto attendant answers business calls with a Company Greeting. A voice prompt then offers callers a menu of options to direct their call by selecting a digit on the dialpad key pad.

Custom Call Routing (CCR)

CCR replaces the Automated Attendant menu with a customized CCR Home Menu to offer callers a wider range of call routing options and access to sub-menus and information messages. CCR allows you to determine the menu options and record the voice prompts that guide callers along call paths.

Audio Messaging Interchange Specification (AMIS) Networking

AMIS Networking includes General Networking parameters, Audio Messaging Interchange Specification (AMIS)-specific parameters and AMIS Site Administration. For more information about AMIS Networking, refer to the *Enterprise Edge Voice Messaging AMIS Set Up and Operation Guide*.

Enterprise Edge Networking

The Enterprise Edge Networking option serves as a link between Enterprise Edge Voice Messaging, Meridian Mail and other voice mail systems at different locations. Enterprise Edge Networking allows the exchange of voice and fax messages between users at different sites on a network connected via Transmission Control Protocol/Internet Protocol (TCP/IP). Enterprise Edge Voice Messaging systems must have Enterprise Edge Networking enabled before receiving or sending network messages. Meridian Mail systems must be equipped with Meridian Mail Net Gateway before receiving or sending network messages. Enterprise Edge Networking uses Simple Mail Transfer Protocol (SMTP) to exchange the messages. For more information, refer to the Configuring networking resources on page 63.

Enterprise Edge Call Center

The Enterprise Edge Call Center application is designed to handle incoming calls efficiently and economically. Incoming calls are distributed to available agents or to Enterprise Edge greetings in your call center. To ensure that each call is handled successfully, the Enterprise Edge Call Center system answers, plays greetings and routes each incoming call to the first available agent in the order of the call's arrival. For more information, refer to the *Enterprise Edge Call Center Set Up and Operation Guide*.

Enterprise Edge Call Center Reporting

Enterprise Edge Call Center Reporting is a Windows software application that provides Real Time statistics and comprehensive management information on the day-to-day performance of your Enterprise Edge system. Enterprise Edge Call Center Reporting helps you manage call traffic and provides a comprehensive range of management reports that provides critical information for accurate business planning. It also has the ability to support multiple Wallboards which can be individually configured to display the information that the agents require. For more information, refer to the *Enterprise Edge Call Center Reporting Set Up and Operation Guide*.

Enterprise Edge Voice over IP gateway

IP telephony is most commonly referred to as Voice over IP (VoIP). VoIP involves the conversion of voice from it’s traditional telephony format into a packet format (digital) that can be transported over an intranet. The Enterprise Edge VoIP gateway allows telephony calls to be made over any intranet connected to the Enterprise Edge system. For more information, refer to the *Enterprise Edge IP Telephony Configuration Guide*.

Enterprise Edge Unified Messaging

Enterprise Edge Unified Messaging consists of three features:

- Enterprise Edge Unified Messaging which allows you to create and receive messages on your personal computer.
- Enterprise Edge Personal Mailbox Manager which allows you to administer mailbox features and functions such as mailbox initialization, recording of greetings, target attendant and the setting up and maintenance of off-premise message notification.
- Enterprise Edge Operator Manager which allows you to change the Operator password, change business status, enable or disable the system attendant and enable or disable the Message Call Answer feature.

For more information, refer to the *Enterprise Edge Unified Messaging Client Installation Guide.*

Enterprise Edge TSP Server

Microsoft's Telephony Application Programming Interface (TAPI) converts industry standard commands passed between Windows and your phone system into a format which both can understand. TAPI consists of a set of programming tools, developed by Microsoft, which provides a standard set of commands that can be used to control any telephone. TAPI allows a Windows application to operate on many different switch platforms with little or no modification. For most telephone systems, a TAPI Service Provider (TSP) is required to use TAPI. For more information, refer to the *Enterprise Edge TSP Server Configuration Guide*.

Enterprise Edge Personal Call Manager

Enterprise Edge Personal Call Manager is a TAPI-based application that provides First Party Call Control for your telephone. For more information, refer to the *Enterprise Edge Personal Call Manager User Guide*.

Enterprise Edge Call Detail Recording

The Enterprise Edge Call Detail Recording software records call activity. Each time a telephone call is made to or from your company, the information about the call is recorded. When the call is completed, information about the call is printed out in Call Records. For more information, refer to the *Enterprise Edge Call Detail Recording System Administrator Guide*.

Nortel Networks Voice Service

Enterprise Edge Attendant Console uses a graphical user interface to provide centralized call management. For more information, refer to the *Enterprise Edge Attendant Console Set Up and Operation Guide* and *Enterprise Edge Attendant Console User Guide.*

Unified Manager

The Enterprise Edge Unified Manager provides a web-based browser that lets you view and change configuration settings for:

- IP Services
- VoIP Service
- Telephony Functions
- Management Server Module
- QoS Module

Most changes made with the Unified Manager become part of current Enterprise Edge programming as soon as you select an item from the menu options. However, some changes won't take effect until about a minute after the user stops programming. If you make a mistake when programming, you will have to reenter the original programming.

For more information, refer to

- Browser requirements on page 26
- Understanding the Unified Manager on page 27
- Enterprise Edge system access on page 30

Browser requirements

The following configuration is recommended for PCs acting as HTTP clients used to configure Enterprise Edge through the Unified Manager.

- Win NT workstation running on P133 or higher CPU (or compatible)
- 64 MB RAM, 10 MB disk space
- Minimum screen resolution of 1024 X 768
- Minimum monitor size of 17 inches

To use Enterprise Edge Unified Manager, you must have:

- Java Virtual Machine (JVM) 5.0 (build 5.0.0.3167 or greater)
- one of the following web browsers:

  Netscape Communicator 4.5 or greater
  Microsoft Internet Explorer 4.0 or greater

If you are using Netscape Communicator, you must set the following parameters:

- Enable Java: On
- Cached document comparison: Every time

If you are using Microsoft Internet Explorer, you must set the following parameters:

- Check for newer versions: Every visit to the page

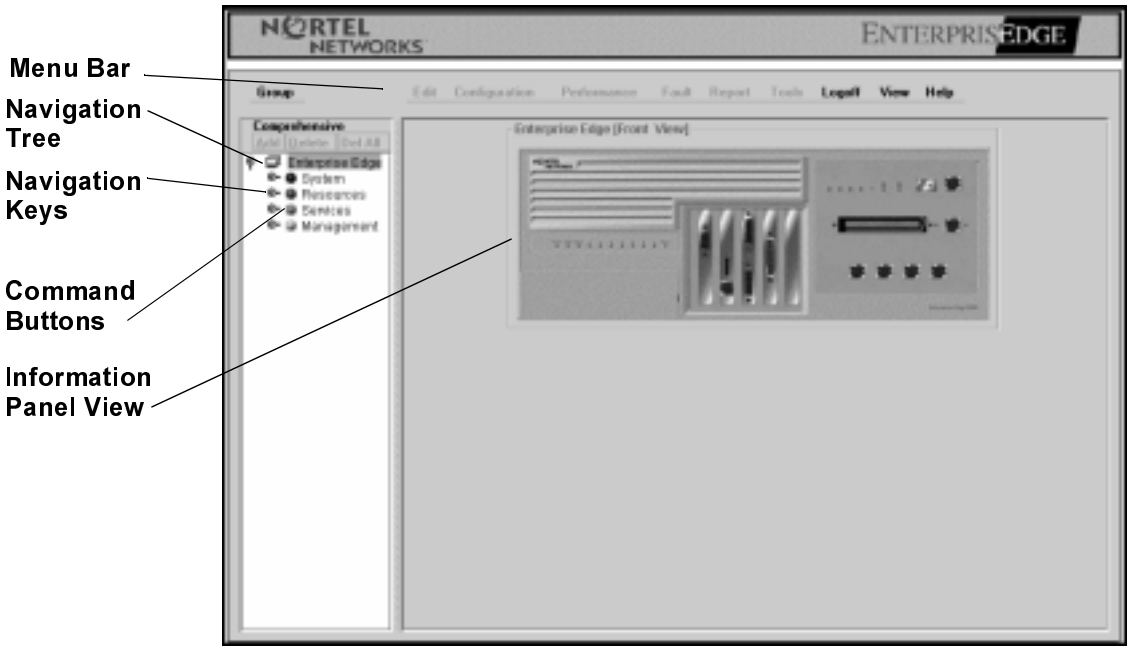
- Java JIT compiler enabled: On

For information about setting these parameters, check the documentation that came with your web browser.

Understanding the Unified Manager

The Unified Manager consists of:

- a menu bar where users access configuration management commands.
- a navigation tree used to navigate between views and configuration windows.
- an information panel view



The menu bar contains configuration management options. These options are enabled when you select the various headings in the navigation tree to enter specific areas of the Enterprise Edge system. If an option is grey, it is not available for the heading you have selected.

The navigation tree contains headings that allow you to access specific areas of the Enterprise Edge system. The key symbol (⚲) beside each heading indicates that the heading can be expanded to show additional headings in the right pane. To make the additional headings appear, double-click the item or just click on the icon itself. As you select various headings in the navigation tree, the heading changes color and the Unified Manager displays the appropriate information panel view.

The information panel can contain configuration windows or dialog boxes indicating the appropriate action and system messages or warnings.

For more detailed information on the Unified Manager, refer to

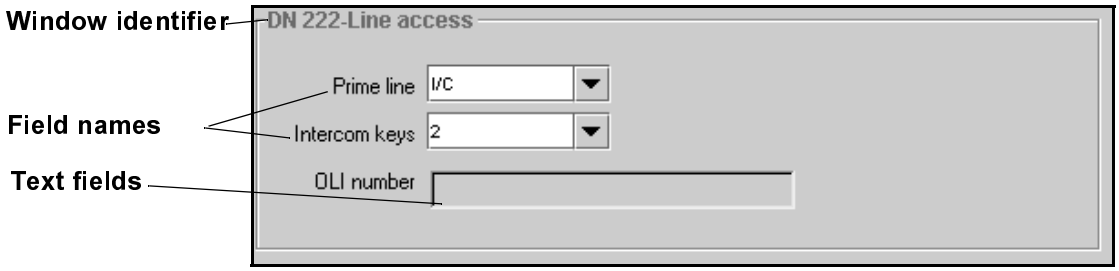
- Using the configuration windows on page 28

- Changing the Unified Manager's appearance on page 28
- Changing data views in the Unified Manager on page 29

Using the configuration windows

The configuration windows are used to configure Enterprise Edge settings. The configuration windows always contain a window identifier. Some fields use edit-in-place formats to allow you to configure settings in the fields opposite each field name. Each time you tab to the next field, the previous field's values are saved. Some fields use drop-down menus to provide you with valid entries for each field.

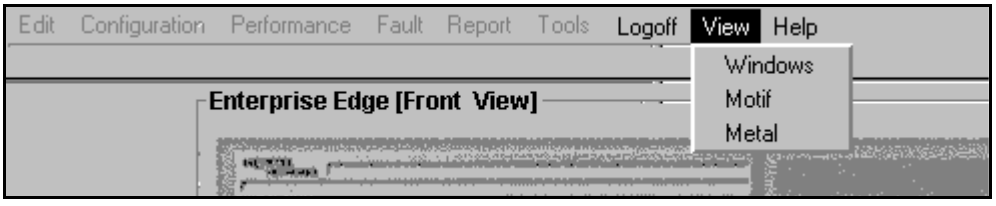
If a value is invalid, an error message appears to alert you of the error. The dialog box format allows you to enter text in fields and save the settings by selecting **Save** or by simply moving to another heading in the navigation tree.



Changing the Unified Manager's appearance

You can change the Unified Manager's display to a Windows, Motif, or Sun Swing appearance using the following procedure.

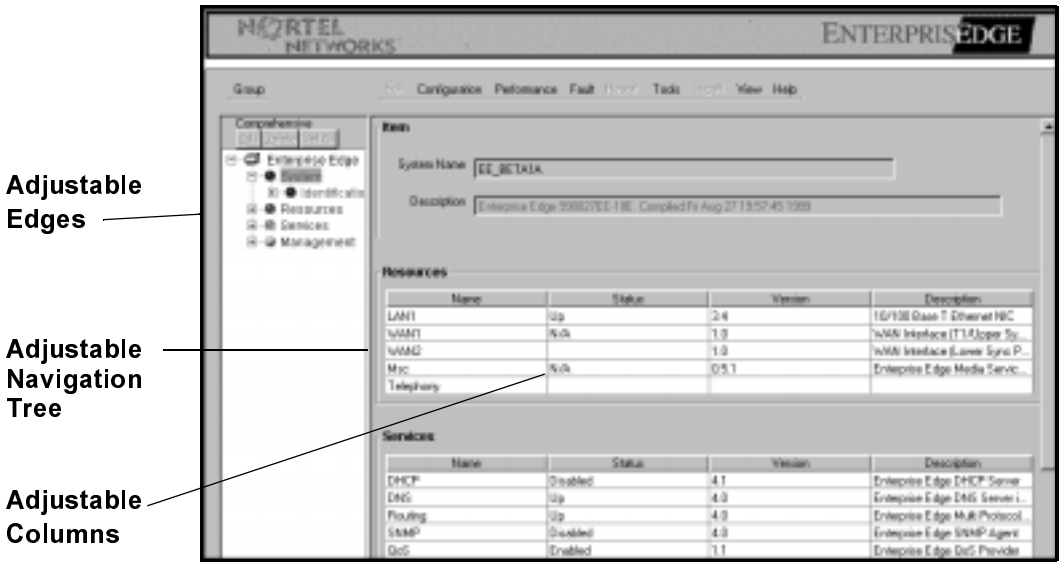
1. Select **View** from the menu bar.
2. Select either **Windows**, **Motif**, or **Metal.**
3. The view is updated for either a Windows, Motif, or default Sun Swing display.



You can resize the Unified Manager and configuration windows using your mouse using the following procedure.

1. Move the pointer over any edge until it changes to a double-headed arrow.
2. Drag the edge of the window to the desired location and release the mouse

.



Changing data views in the Unified Manager

You can change the order and size of data views in the Unified Manager.

Use the following procedure to change the column order.

1. Point to the column that you want to move and click on it with your mouse.

2. Holding the mouse down, drag and drop the column to the appropriate location.

   The other column, already in this location, automatically changes places with the column you are moving.

Use the following procedure to change the column width.

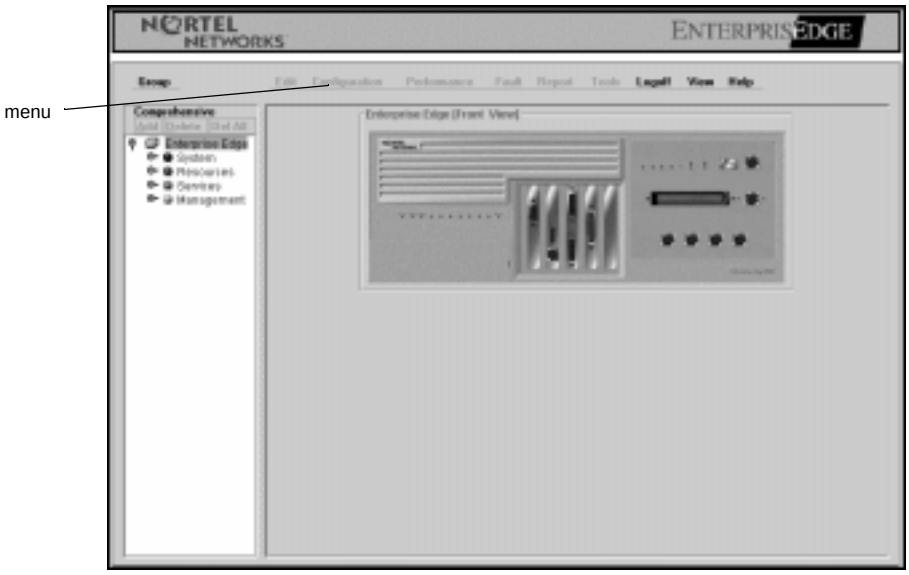
1. Keeping the pointer in the heading row, move it over any column edge until it changes to a double-headed arrow.

2. Pull the column edge to the appropriate location.

Menu descriptions

You access Enterprise Edge functions using the menu. The menu is dynamic which means that the menu commands change depending on the action a user takes.

Enterprise Edge menu



Menu descriptions

Use	To
Group	View the system, resources, services, and management.
Edit	Edit parameters.
Configuration	Access configuration dialog boxes and screens
Performance	Access performance graphs and tables.
Fault	Access fault management settings.
Report	Generate a report.
Tools	Use Enterprise Edge tools.
Logoff	Log off the Enterprise Edge server.
View	Change the appearance from Windows, Motif or Sun Swing.
Help	Access online help.

Enterprise Edge system access

Note: User access must be controlled by providing one userid, the administrator, with read-write privileges. All other users must be given read-only privileges. This prevents concurrent configuration of the Enterprise Edge system.

The Unified Manager's navigation tree contains four main headings that allow you to access specific areas of the Enterprise Edge system. The main headings are:

- System on page 31
- Resources on page 31
- Services on page 31
- Management on page 31

System

The options under the **System** heading allow you to view system settings. When you select the **System** heading, the menu options **Configuration**, **Performance** and **Fault** are enabled. These menu options provide access to statistical information and allow you to enable or disable services. For more information on configuring your system settings, refer to the Configuring system settings on page 57. For information on Performance and Fault monitoring, refer to Viewing system performance and fault alarms on page 283 and Enterprise Edge system diagnostics and utilities on page 241.

Resources

The subheadings under the **Resources** heading, allow you to configure the following resources:

- LAN
- WAN
- Msc
- Telephony

For more information on LAN and WAN programming, refer to Configuring networking resources on page 63. For more information on MSC and Telephony programming, refer to Configuring Telephony Resources on page 77.

Services

Use the options under the **Services** heading to configure services for the Enterprise Edge system. For more information on configuring these settings, refer to Configuring Enterprise Edge Services on page 185.

Management

Use the options under the **Management** heading, to configure network management parameters. For more information on configuring these parameters, refer to Configuring Management Settings on page 229.

Using Enterprise Edge Services 3

This chapter includes information on:

- IP routing
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name Server (DNS) Service
- Web Caching/Proxy
- Simple Network Management Protocol (SNMP)
- Quality of Service (QoS)
- Using Traffic Filters
- Using Protocol Prioritization Queues
- LAN Connections
- WAN Connections

Routing and IP services supported by Enterprise Edge

Enterprise Edge supports the following routing and IP Services:

- Routing Services
  - IP Routing Protocol
  - RAS Service and Dial In Capabilities for Management Purposes Only
  - RIP
  - Packet Filtering
- IP Services:
  - DHCP
  - DNS
  - Web Caching
- VoIP (voice over IP) Service

IP Routing

This section includes information on:

- IP Routing Overview
- Enterprise Edge IP routing specifics
- IP addressing overview
- Static routing
- Routing Information Protocol (RIP)
- Packet Filtering
  - source address
  - destination address
  - IP Protocol ID
  - TCP Port
  - UDP Port
  - ICMP Type
  - ICMP Code
- LAN to WAN routing
  - managing traffic using Interrupt Modulation
- LAN to LAN routing
  - Fast Path Routing

IP Routing Overview

The Internet Protocol (IP) is the protocol used on the Internet to send data from one computer to another. Each computer on the Internet, called a "host", has at least one address that identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail or a web page), the message gets divided into units called packets. Each of these packets contains both the sender's Internet address and the receiver's Internet address.

A packet is first sent to a router that reads the destination address and forwards the packet to an adjacent router that reads the destination address.This routing process continues across the Internet until one router recognizes the packet as belonging to a computer in its immediate neighborhood, or domain. That router forwards the packet to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than the order they are sent. Another protocol, the Transmission Control Protocol (TCP) puts the packets in the right order.

IP is a connectionless protocol, which means that there is no established connection between the end points that communicate. Each packet that travels through the Internet is treated as an independent unit of data without any relation to another unit of data. The packets get put in the right order because TCP, the connection-oriented protocol, keeps track of the packet sequence in a message. In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

Enterprise Edge IP routing specifics

Using Enterprise Edge Unified Manager, you can perform the following routing configuration options:

- Add or delete the interfaces to routing protocols
- Configure routing protocol options
- Add and delete static routes
- Add or delete filters
- Set filter actions

For instructions on configuring routing options, see Routing on page 192.

The followings table shows the Enterprise Edge IP routing protocols and the precedence order when conflict or redundant routes occur.

Precedence	IP Routing Protocols
1.	Static Routing
2.	SNMP
3.	RIP v1 and v2

IP Addressing Overview

IP addresses follow the format nnn.nnn.nnn.nnn, where nn is a number between 0 and 255, for example, 192.123.4.56 or 10.1.1.1. IP addresses enable computers to communicate to each other. Both servers and workstations on a network must have IP addresses. There are two types of IP addresses:

Dynamic – A dynamic IP address changes. Dynamic IP addresses are assigned to computers by an IP address server as the computer needs it. Usually there is a particular range or scope of IP addresses that your network uses. With dynamic IP addressing, a computer can have a different IP address every time it connects to the network. Other devices must know the computer's IP address so that they can communicate with it. The IP address server manages the assignment of IP addresses to the client workstations.

Static – A static or fixed IP address never changes. It is assigned to a computer permanently. The computer has the same IP address every time it connects to the network and is known to other devices on the network by that IP address.

Static Routing

Enterprise Edge users can add static routes to the IP routing table. These static routes take precedence over those routes chosen by routing protocols, such as RIP.

To add a static route, see Static Route on page 198.

Note: Make sure that users do not add a static route for default route 0.0.0.0 with mask 0.0.0.0. Enterprise Edge's Net Link Manager automatically creates a default route and adjusts it according to link status unless router or Net Link Manager are running.

Routing Information Protocol (RIP)

RIP is a widely-used protocol for managing routing information in a self-contained network, such as a corporate intranet. RIP is classified by the Internet Engineering Task Force (IETF) as one of several internal gateway protocols (IGPs).

A RIP router sends full updates, which list all the other hosts it knows about, to its closest neighbor host every 30 seconds. The neighbor host sends the information to its next neighbor, until all the hosts in the network know the routing paths, a state known as network convergence. RIP uses a hop count to determine network distance. Each host with a router in the network uses the routing table information to determine the next host for the packet, until a specified destination is reached.

Enabling RIP on Network Interfaces

To run RIP on one or more network interfaces, go to the specific interface under router and enable RIP. After you enable RIP for an interface, you do not have to reboot the Enterprise Edge server for the changes to take effect.

Packet Filtering

A packet is a unit of data routed between an origin and a destination on the Internet or on any other packet-switched network. When any file such as an e-mail message, HTML file, GIF file, or URL request is sent on the Internet, the IP layer divides the file into packets of an efficient size for routing. Each of these packets is numbered and includes the Internet address of the destination.

Enterprise Edge supports basic (or stateless) packet filtering for IP. You can configure the filter to pass only the packets from the routes they list, or to pass everything except the packets for the routes they list.

Each route in the list can be any combination of the following packet filtering features. By default, no packet filter is configured.

Enterprise Edge supports the following packet filtering features for IP:

Packet Filter Feature	Comments
Source Address	The source address field of the packet to be filtered.
Source Mask	The source address mask of the packet to be filtered.
Destination Address	The destination address field of the packet to be filtered.
Destination Mask	The destination address mask of the packet to be filtered.
Protocol	The protocol type of the packet to be filtered.
Source Port	The source port of the packet to be filtered. This field applies only if protocol value is TCP or UDP.
Destination Port	The destination port of the packet to be filtered. This field applies only if protocol value is TCP or UDP.
ICMP Type	The ICMP type field of the packet to be filtered. This field applies only if protocol value is ICMP.
ICMP Code	The ICMP type field of the packet to be filtered. This field applies only if protocol value is ICMP.

Note: When you set filters, you must forward packets going to the RPC port (port 135 TCP or UDP) for correct Unified Manager operation.

LAN-to-LAN Fast Path Routing

Enterprise Edge provides an optional, second, 10/100 LAN interface. If the second LAN interface is used, Enterprise Edge uses optimized software for high performance routing. This includes an innovative design that speeds up the performance for LAN-to-LAN routing by over three times the rate that is normally achieved with traditional software architecture.

Dynamic Host Configuration Protocol (DHCP)

DHCP (Dynamic Host Configuration Protocol) is a protocol that lets network administrators manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocols (TCP/IP), each machine that connects to the Internet needs a unique IP address. If an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine.

Without DHCP, the IP address must be entered manually at each computer. If computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address if a computer connects to a different place in the network.

You can set up Enterprise Edge to be your LAN’s DHCP server and let it assign IP addresses to the workstations on your LAN as necessary. This is the recommended configuration.

If you set up the Enterprise Edge server as a DHCP server, you must let all of your workstations know that they will have their new IP addresses assigned by Enterprise Edge. To do this, you may need to change the configuration of each workstation individually.

If you already have a DHCP server, you must let it know that the Enterprise Edge server is their gateway and DNS proxy for the workstations.

Your Enterprise Edge server can function as a DHCP server. You can use this feature if you do not want to administer static IP addresses for every workstation on your network. You can configure Enterprise Edge to assign IP addresses dynamically.

Automatic Configuration using a DHCP server

To configure the DHCP server, you must define a particular range (or scope) for each LAN interface in Enterprise Edge and allocate a block of IP addresses for that scope. The Enterprise Edge Auto-Configure system automatically creates a scope using parameters inherited from the LAN interface.

Guidelines for Using DHCP

Since many default DHCP parameters are inherited from LAN interface parameters, configure LAN interfaces before configuring DHCP.

If you are modifying the DHCP configuration on Enterprise Edge, follow the same guidelines of your organization. In particular, you can perform one or more of the tasks listed below to ensure proper operation of the networked system:

1. If a change in the DHCP configuration resulted in the change of ‘Router’ and ‘Subnet mask’ options in a scope, users must do one of the following to ensure basic operation:
   - Execute *ipconfig/release* and *ipconfig/renew* on each of the workstations. For Windows 95 and Windows 98, use its equivalent, *winipcfg*.
   - For clients that do not support *ipconfig* and *winipcfg*, reboot is required to renew their IP addresses.

2. If a change occurs in the DNS server or DNS name options, users must repeat the tasks in step 1 to ensure proper connectivity with the organization.

3. Always schedule a down time associated with these changes.

4. Nortel Networks recommends that you reboot Enterprise Edge to initialize changes.

Using Enterprise Edge, you can define a DHCP scope for each LAN interface. DHCP server parameters are divided into two categories: global and scope specific. Global parameters apply to all scopes. Specific parameters apply to a specific scope.

Domain Name Service (DNS)

The domain name service (DNS) is the system within the Internet that maps names of objects, usually host names, into IP numbers or other resource record values. The name space of the Internet is divided into domains. The responsibility for managing names in each domain is usually delegated to systems in each domain.

Enterprise Edge functions as both a gateway to the Internet and as a DNS proxy:

- **Gateway**: a system that links two different types of networks and enables them to communicate with each other. Enterprise Edge is the gateway that links your company's network to the Intranet or Internet. Depending on your configuration, you can let your workstations know that Enterprise Edge is your Internet gateway.

Note: If your PC is a DHCP client under Enterprise Edge, you do not have to let your workstations know that Enterprise Edge is your Internet gateway.

- **DNS Proxy** – A Domain Name Service (DNS) proxy translates alphabetic domain names into computer-readable IP addresses. For example, the domain name www.nortelnetworks.com for the Nortel Networks web site can translate to the IP address 192.177.5.18. After a domain name is translated into an IP address, the workstations on your network can communicate with the web site. Depending on the configuration of your system, you can let your workstations know that Enterprise Edge is the DNS proxy.

Note: If your PC is a DHCP client under Enterprise Edge, you do not have to let your workstations know that Enterprise Edge is your DNS server.

When Enterprise Edge receives DNS requests from clients, it first checks its local cache for name entries and records. If found locally, Enterprise Edge immediately responds to clients. Otherwise, Enterprise Edge creates a new DNS request to the remote Primary or Secondary DNS servers on behalf of the client. If the remote DNS server responds with the requested records, they are forwarded to clients and cached in Enterprise Edge.

Guidelines for Using DNS

Consider the following guidelines when using DNS:

- If the Enterprise Edge DNS service is enabled, make sure that clients always use Enterprise Edge as their DNS server.
- When it is disabled, set the DNS Server field in DHCP configuration to the remote DNS server IP address. If DHCP service is also disabled in Enterprise Edge, tell all clients to set the DNS server in their IP configuration to the remote DNS server.
- The DNS proxy carries security features because it keeps all of the internal IP addresses from external web servers.
- You are required to fill in the remote Primary DNS server IP address. See DNS settings on page 192 for instructions.

Web Caching/Proxy

When you use Enterprise Edge as a web proxy, Enterprise Edge can store, or cache, information downloaded from the Internet. A proxy is a server that acts on behalf of another. Web caching allows LAN workstations to share common information downloaded from the Internet.

Data is usually cached on individual workstations. Each time a workstation on the LAN requests information from the Internet, the individual's request is sent to the Internet, and the information is returned to their workstation. If multiple LAN workstations request common data, a web cache on the network reduces download time from the Internet.

With Enterprise Edge configured as a web proxy with web caching:

- LAN workstations have shorter download times.
- Previously downloaded information is stored for future use by all workstations on the LAN.
- Enterprise Edge retrieves information from the Internet only if it is not already cached or if the cached file is out of date compared to the information on the Internet.
- "Cookie" blocking protects users' privacy.

You can configure the web caching settings through your web browser.

The web proxy also provides security features similarly to the DNS proxy because it hides all of the internal browsers' IP addresses from external web servers. External web servers see only Enterprise Edge's IP address.

Guidelines for Using Web Caching/Proxy

The Enterprise Edge web proxy uses a web server for running in HTTP-Proxy mode.

Consider the following guidelines when using web caching/proxy:

- A web server installed in Enterprise Edge cannot be used as a general purpose HTTP server. It is only used by the Enterprise Edge web-based management client and web-cache services.
- If users must run their web sites, they must run the HTTP Server on another system and make its IP address known to Enterprise Edge.

To set the web server as the web cache/proxy, refer to Web cache on page 216.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is the protocol that governs network management and the monitoring of network devices and their functions.

Guidelines for Using SNMP

Consider the following guidelines when using SNMP:

- You can set read-only and read-write community names.
- You can set a list of permitted managers. When set, the agent responds to requests from SNMP managers from only those IP hosts.
- An empty list of permitted managers implies that agent responds to requests from anyone.
- You can set trap communities. Each trap entry identifies the community name that must be used and the manager addresses.
- You can enable or disable sending authentication traps.
- You can enable or disable the SNMP agent.
- At present, SNMP supports only MIB-II (RFC 1213) MIBs.

Quality of Service

This section includes information on:

- QoS overview
- DiffServ networks
- Legacy networks
- Admission control
- Packet marking for DiffServ networks
- Port range setting for legacy networks
- Relationship between the QoS Module and the VoIP QoS monitor
- Enterprise Edge QoS restrictions and defaults

QoS overview

On the Internet, Quality of Service (QoS) is the methodology by which transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is a concern for the continuous transmission of high-bandwidth voice and video multimedia information. Transmitting this content dependably is difficult in public networks using ordinary “best effort” protocols.

Real-time applications that include voice and video are time-sensitive. Delivering voice and video over the Internet requires control of packet delay and jitter. Differentiated Services (DiffServ) is a QoS framework standardized by IETF that focuses on DiffServ standards for real-time and mission critical applications. The DiffServ standards are evolving and vendors are starting to develop network devices that support DiffServ.

The purpose of the Enterprise Edge QoS module is to prioritize IP traffic and to provide an acceptable quality of service to delay and jitter sensitive applications such as audio and video as well as mission critical applications.

The Enterprise Edge QoS module serves two primary purposes:

- In a DiffServ network, it acts as an edge device and performs the packet classification, marking, and prioritization.
- In a non-DiffServ or legacy network, it manages the WAN link to make sure premium voice (and optional video) packets get high priority when crossing the slow WAN link in both directions.

DiffServ Networks

For DiffServ networks, Enterprise Edge:

- Intercepts all H.323 traffic
- Identifies call setup packets
- Performs admission control based on the WAN link usage
- Marks the packets as premium once admitted

Enterprise Edge implements the DiffServ queuing model that includes a premium queue and eight best-effort queues. The premium queue has a stricter high priority than the best-effort queues. The eight best-effort queues are scheduled by a weighted-fair-queuing (WFQ) algorithm. Since best-effort traffic is not shaped and does not go through the admission control process, the WFQ is needed to avoid starvation of low priority packets.

Currently, H.323 traffic is allowed to get into the premium queue. Users can allow other traffic to be premium by setting up priority filters on the web-based GUI using the following filter criteria:

- Source IP address (with mask)
- Destination IP address (with mask)
- IP protocol ID (e.g. TCP, UDP, or ICMP)
- Source port range
- Destination port range
- Incoming TOS field

Note: There is no traffic shaping mechanism implemented in this release of Enterprise Edge. Be cautious when setting up premium priority filters. If the traffic is high volume and with high bursts, it can impact VoIP quality. Unless necessary, Nortel Networks recommends that you allocate traffic to the high priority best-effort queues instead of the premium queue.

Legacy Networks

In a legacy network, Enterprise Edge assumes that network devices, such as routers and switches, do not recognize the IP header TOS field (as defined by DiffServ) and do not perform the corresponding priority processing. However, most of the current installed routers, including those from Cisco and Nortel Networks, allow administrators to set up priorities by IP addresses, port numbers, or protocol types, which is similar to the priority filters described above.

Note: This information is specific to H.323 traffic in legacy networks.

In this environment, Enterprise Edge allows H.323 voice (and optional video) packets to travel across the WAN link with high priority in both directions using existing router features.

An administrator must reserve a block of UDP port numbers and configure them as high priority in both Enterprise Edge and the remote router at the other end of the WAN link. Enterprise Edge forces all of the admitted H.323 streams to fall into the reserved port range by using a proprietary technique so that these H.323 voice (video) packets can get high priority. This is completely transparent to the end H.323 terminals.

See Appendix C: Setting Up Remote Routers on page 349 for additional information on setting UDP port ranges for remote routers.

Note: If an administrator configures all routers in their corporate network with the same reserved port numbers (both in and out), admitted H.323 streams can get end-to-end high priority. However, routers connected to WAN links are more critical, because WAN links are typically the bottlenecks.

You can set up best-effort traffic priorities through the web-based Unified Manager by using the following filter criteria:

- Source IP address (with mask)
- Destination IP address (with mask)
- IP protocol ID (e.g. TCP, UDP, or ICMP)
- Source port range
- Destination port range
- Incoming TOS field

There are a total of 8 priority classes for best-effort traffic in Enterprise Edge. By default, all best-effort traffic is sent to Class 5 (queue 5), with Class 1 the highest and Class 8 the lowest in priority.

Admission Control

Enterprise Edge allows users to set a certain percentage of the WAN bandwidth for premium traffic. This traffic takes strict priority over best-effort traffic. In this version, H.323 (VoIP) flows need to pass the admission control process to be treated as premium traffic.

For admission control, Enterprise Edge uses the WAN Premium Bandwidth parameter. Specifically, for each H.323 flow, QoS performs admission control using the negotiated coding algorithm. A flow is admitted as a premium flow if the current total WAN premium usage plus the new flow is lower than the allocated WAN premium bandwidth. Otherwise, the flow is rejected and the flow is still delivered as best-effort traffic.

As a reference point, for a typical G.729 codec, each VoIP flow requires the following WAN bandwidth, depending on the codec sample rate:

G.729	Sample Rate 30 ms	Sample Rate 20 ms	Sample Rate 10 ms
No Compression	10.6 k	14 k	24 k
Data Compression	8 k	10 k	16 k
RTP Hdr Comp.	5.8 k	6.8 k	9.6 k

Note: The calculation is based on a full-duplex WAN link with HDLC overhead and VoIP with silence suppression.

Nortel Networks recommends that for slow WAN links, such as a 56K leased line or ISDN, H.323 video is not configured as premium traffic.

Packet Marking for DiffServ Networks

Enterprise Edge classifies traffic and marks packets by setting the IP header type of service (TOS) field. By default, the following items are classified as premium traffic:

- All VoIP flows
- RIP packets: routing packets are periodically exchanged between Enterprise Edge and remote routers. These packets need higher priority than regular packets to ensure that the routing protocol is working properly.
- ICMP packets: Enterprise Edge Net Link Manager uses the ‘ping’ command to determine whether the primary WAN link is active or inactive. These packets are not delayed by regular packets.
- UDP Port 5000 packets – Enterprise Edge VoIP QoS Monitor uses port 5000 in a proprietary protocol to monitor the IP network delay and jitter. Because Enterprise Edge assigns VoIP packets to the premium queue, it also gives these monitor packets high traveling priority.
- Admitted RTP/RTCP packets.

In Enterprise Edge, there are two places a user can set up a TOS field in an IP header:

TOS-for-Premium-Traffic – this field sets TOS bits for premium packets for DiffServ networks. If this field is ignored, Enterprise Edge uses a default value of 0xB8.

TOS-for-Priority-Filters– this field sets TOS for those packets matching a specific priority filter.

Note: You can specify packets matched to a filter to go Priority Queue 0 – 8. Queue 0 is for premium packets, and Queue 1 – 8 correspond to best-effort priority classes 1 – 8.

If you specify Queue 0 and a TOS bits for a filter, then this TOS takes precedence over the TOS set for premium traffic for all packets that match this filter.

The default TOS for all best-effort packets is 0x00, and the default queue for best-effort packets is Queue 5.

WARNING
Premium flows that are specified by priority are not admission controlled. Unless you know the behavioral characteristics of a flow, do not specify flows as premium. Instead, you can specify them as the highest B-E traffic.

Consider the following guidelines when you set up priority filters

- The fewer the conditions to check for, the fewer CPU cycles are consumed. Filter processing is faster if fewer conditions are specified, without compromising the precision in selection.
- If you don't need the value of a particular criterion, such as source port number, don't set a corresponding value for the filter.
- When you specify the layer 3 sub-protocols, use the port number/IP address combinations and avoid specifying the protocol field. Nortel Networks recommends that you specify a protocol field only if you manage an unusual condition in your network. This reduces the consumption of CPU cycles.
- Users can configure the precedence of the filters. Packets are matched against each filter sequentially until a match is found. Pay attention when specifying the precedence of filters. Placing 'popular' filters ahead of 'unpopular' filters can significantly speed up the processing.

Port Range Setting for Legacy Networks

Enterprise Edge uses UDP port ranges to provide high priority to VoIP packets in existing legacy IP networks. These same port ranges must be reserved and set to high priority on all routers that an administrator expects to have QoS support. Reserving port ranges is not required for DiffServ networks.

You can select any port ranges that are not used by well-known protocols or applications.

Each H.323 or VoIP RTP flow uses two ports. The total number of UDP port numbers to be reserved depends on how many concurrent RTP flows are expected to cross a router interface. In general:

- Backbone routers reserve more ports than edge routers.
- Edge routers' port ranges are a subset of the backbone router port ranges.
- Add UDP 5000 to high priority.
- Enterprise Edge's port ranges are a subset of the remote router's port ranges.
- You must reserve two ports for each voice call you expect to carry over the WAN. You need two ports for each video session if it is given premium treatment.
- You can reserve multiple discontinuous ranges. Enterprise Edge requires that each range meet the following conditions:

  - Each range must start with an even number.

  - There must be an even number of ports in a range.

See Appendix C: Setting Up Remote Routers on page 349 for additional information on setting UDP port ranges for remote routers.

Relationship between the QoS Module and the VoIP QoS Monitor

The VoIP gateway in Enterprise Edge includes a Quality-of-Service Monitor (QMON) that periodically monitors the delay and jitter of IP networks between two peer gateways by using a proprietary protocol. These monitoring packets are delivered at UDP port 5000.

The main objective of the QMON is to allow new VoIP calls to fall back to the PSTN if the IP network is detected as “bad”.

The QoS module discussed here complements QMON. While QMON passively monitors the IP network, the QoS module actively improves the IP network by giving VoIP packets higher priority to travel so that the chance for QMON to detect “bad” is reduced.

Note: For a VoIP call, if a packet passes QMON but fails the QoS admission control, it is delivered over IP but only as a best-effort flow. There is no fallback to PSTN if a packet has passes QMON checking.

QMON packets travel at the same priority as VoIP packets, or at higher priority than normal IP packets. If VoIP packets travel at a premium level but QMON packets travel at normal best-effort level, it is possible for QMON to report the IP network as “bad” and start fallback to the PSTN, but the actual delay and jitter for VoIP packets are still “good”, since VoIP packets have a higher priority. To avoid this, add UDP port 5000 to the high priority queue in all routers.

Enterprise Edge QoS Restrictions and Defaults

Enterprise Edge QoS includes the following restrictions and defaults:

- By default, the general bulk of traffic (not defined by priority filters) is routed to best-effort Queue 5 (with Queue 1 the highest priority and Queue 8 the lowest). An administrator can define four classes of traffic above the generic traffic and three classes below it.
- A maximum of 31 priority filters for best-effort traffic can be created.
- The QoS module can be ON or OFF. The default setting is ON.
- The predetermined WAN bandwidth is always available to VoIP gateway channels. That is, VoIP gateway calls are always admitted. The remaining WAN premium bandwidth can be used by other H.323 streams, such as Microsoft NetMeeting. If there is no VoIP gateway traffic, the VoIP WAN bandwidth can be used only by best-effort traffic, not other premium traffic (for example, Netmeeting). Enterprise Edge does not support preemption of admitted premium streams.
- Currently, packet prioritizing and priority filters apply only to outbound traffic for specified interfaces. Inbound traffic is treated on a first in/first out (FIFO) priority.
- The maximum port numbers a user can reserve for premium traffic is 256.

LAN Connections

The Enterprise Edge Ethernet / 802.3 interface supports the IEEE 802.3 Ethernet frame format. The Ethernet interface uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to manage the access to the physical media.

The Enterprise Edge Ethernet interface supports the following features:

- 100 BASE – TX with RJ-45 connector
- 10 / 100 Auto Sense
- Full Duplex support
- Fast LAN-LAN routing

WAN Connections

This section includes information on:

- WAN overview
- Permanent WAN connections:

  – Frame Relay

  – PPP

WAN overview

A WAN (wide area network) is a geographically dispersed data communication network. The term WAN distinguishes a broader data communication structure from a local area network (LAN). A WAN can be privately owned or rented, but usually connotes the inclusion of public (shared user) networks.

Enterprise Edge includes two primary WAN links (WAN1, WAN2) and a backup WAN dial up link (WAN3).

- The Primary WAN link is always a permanent link and it is a dedicated network adapter. The primary link runs either Frame Relay or the PPP protocol at the link layer.

  The Enterprise Edge primary WAN connection is through a two-port card. These two ports can be independently configured to run Frame Relay or PPP. The card includes one serial sync port and one T1 port.

- The backup WAN link is always configured as dial-on-demand network adapter by the router. The backup Wan link runs PPP only. Enterprise Edge provides backup WAN connection through a V.90 modem.

  The primary and backup link management is performed from Enterprise Edge. There is a Net Link Manager running in Enterprise Edge that monitors the primary link status and it starts the backup link when a break in the primary link is detected. Similarly, the backup link is automatically terminated when the primary link becomes active.

Note: Net Link Manager can back up only one link, even though there are two primary links. Net Link Manager backs up the link whose next hop address is given to it.

- Net Link Manager manages the default route in Enterprise Edge. If a link breaks, Net Link Manager removes all the default routes on the broken link and adds the default route to the new link. This happens during switch over from primary to secondary links and vice versa.

Permanent WAN Connections

This section includes information on the following topics:

- Frame Relay
- PPP

The permanent WAN connections are provided by a WAN card that supports PPP and Frame Relay connections. Each port can be configured to run either of the protocols independently.

The WAN cards are provided with one T1 port (with in-built CSU/DSU) and one serial sync port or dual serial sync port versions.

The Enterprise Edge serial sync port supports the following:

- Interfaces: V.35, RS442, RS 323, X.21
- Maximum line speed:8 Mbit/sec

Frame Relay

Enterprise Edge supports Frame Relay in *group* mode. That is, for each physical port (serial sync or T1 port), there is one IP address for all PVCs.

The available DLCI numbers are 0-1023, of which 16 are reserved. The maximum number of PVC’s allowed is 1008.

For a Frame Relay network, Enterprise Edge supports the Frame Relay Forum standard FRF.9 compression protocol with the standard STAC compression algorithm.

Software performs the compression, which can be enabled or disabled by using Unified Manager.

PPP

Point-to-Point Protocol (PPP) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider can provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP). PPP is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP can process synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection.

PPP on the primary WAN link uses synchronous point-to-point communication. Because the physical media is point-to-point, authentication attributes are not supported in this mode.

Enterprise Edge supports PPP Compression Control Protocol (CCP) (RFC 1962) with STAC compression algorithm.

This compression is done by software and can be enabled or disabled by using a parameter in PPP configurations.

Backup Up WAN Connection

In Enterprise Edge, the back up WAN connection is a V.90 modem that is used as a dial-up WAN link.

The modem is provided through an RJ-11 connector. The modem has the following features:

- V.90 56 kbps ITU standard
- V.34 33.6 kbps ITU standard
- V.42/MNP 2-4 error control
- V.42 bis/MNP 5 data compression
- Compatible with ITU and Bell Standards from 56 kbps down to 1200 bps

Note: The modem is capable of receiving at up to 56 kbps and sending at up to 31.2 kbps. Because of FCC regulations, receiving speeds are limited to 53 kbps. The actual speed can vary, depending on factors such as current line noise.

Backup WAN Links

Enterprise Edge supports Microsoft Point-to-Point Compression (MPPC), and RFC 2118 for traffic across dial-up links. The compression ratio of MPPC is approximately 4 or 5 to 1.

For the remote backup, Enterprise Edge supports the following authentication mechanisms:

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP). This protocol is a more secure procedure for connecting to a system than the PAP. The system attempts CHAP before using PAP.

  Software data compression on backup/dial up link is an optional feature in Enterprise Edge. The default is set to ENABLE data compression.

Note: Remote user dial-in as an RAS client is supported for administrative purposes only.

Guidelines for Using Remote Dial-in

Consider the following guidelines when using remote dial in:

- The same modem is shared between the remote dial-in for administration and the backup WAN link. If a remote administration user is connected while the primary link breaks, the automatic backup function does not occur.
- While using the back-up interface, Enterprise Edge always calls. Enterprise Edge does not answer an incoming call from a router.
- Support for callback configuration is not provided.

Setting up your Enterprise Edge system 4

Refer to the following information when setting up your Enterprise Edge system.

- Enterprise Edge required parameters on page 53
- Setting up an Enterprise Edge IP Address on page 54
- Setting up web-based administration on page 55
- Logging on to Enterprise Edge on page 56
- Logging off Enterprise Edge on page 57
- Rebooting the Enterprise Edge server on page 57
- Configuring system settings on page 57

Enterprise Edge required parameters

The Enterprise Edge quick start module provides quick access to the parameters necessary for the Enterprise Edge server to become active online. However, you must enter a minimum set of parameters within the quick start module. For more information, see the *Enterprise Edge Installation Guide*.

Obtain the required parameter values from an Internet Service Provider (ISP) or corporate network administrator.

Note: Nortel Networks recommends that after you powered on the Enterprise Edge server and connect with either an RS-232 or an Ethernet port, configure all the required parameters at the same time. After you configure the parameters, reboot the Enterprise Edge server from either the console or the graphical user interface (GUI).

Users must enter the following parameters:

- Initial IP and mask for all network interfaces
- Primary (and optional secondary) DNS servers
- Default next-hop router
- Fractional T1 channel numbers (if you are using fractional TI)
- System name
- WAN Link Protocol
- Frame Relay DLCI / CIR (if applicable)
- V.90 modem dial-up username and password (if applicable)
- V.90 modem dial-up phone number and optional alternate phone number (if applicable)

The following table describes the Enterprise Edge server connectivity options.

Field	Definition
HTTP	You can launch your JAVA-enabled browser to connect to the Enterprise Edge server IP address that connects to your PC. This displays the log in screen. See the Enterprise Edge login screen on page 56.
TTY	You can connect a dumb terminal to the console of the Enterprise Edge server through an RS-232 cross-over cable, or you can use Hyperterminal from Win95/ Win NT systems. Refer to the installation guide for console menus.

Setting up an Enterprise Edge IP Address

To manage the Enterprise Edge server using a web browser or a Telnet connection, you must first set up the IP address. The Enterprise Edge server LAN interface is shipped with default IP 10.10.10.1 and mask 255.255.255.0.

To set up the Enterprise Edge server initial IP address using a RS-232 port:

1. Turn on the Enterprise Edge server power switch.
2. Connect a PC or laptop computer to the Enterprise Edge server RS-232 port.
3. Start a hyperterminal on the PC or laptop computer.
4. Enter the LAN/WAN IP address and other parameters.

To set up the Enterprise Edge server IP address using a LAN:

1. Turn on the Enterprise Edge server power switch.

2. Connect a laptop to the Enterprise Edge server by Ethernet (back-to-back by using a crossover cable to avoid disturbing the corporate LAN).

3. Set your PC or laptop computer IP address to 10.10.10.2 with a mask 255.255.255.0.

4. Start a web browser on your laptop with a URL of 10.10.10.1.

Setting up web-based administration

To establish web-based administration, a workstation must be set up as an Enterprise Edge client with Internet Explorer 4.0 or greater and a JAVA Virtual Machine (JVM) 5.0.0.2922 or greater installed.

To install JVM on a workstation, search the Microsoft information web page for instructions.

These minimum PC requirements are discussed in Enterprise Edge specifications.

Note: The ideal display for a monitor attached to Enterprise Edge is 1280 x 1024.

Browser settings

Set your browser as follows:

Program	Required Settings
Netscape Communicator 4.5 or greater	Click Settings: Edit: Preferences Category Advanced set Enable Java: On set Category: Cache set Cached document comparison: Every Time
Internet Explorer 4.0 or greater	Choose Views: Internet Options Category: General: Temporary Internet Files: Settings click Check for newer versions of stored pages: Every visit to the page set Advanced Java VM set Java JIT compiler enabled

Enterprise Edge OA&M allows multiple users to log on. If each user that logs on attempts to configure the same or related subsystems, the most recent modification remains in effect and overwrites changes by another administrator. Administrators must be careful to not make any unintended changes.

Nortel Networks recommends that only one administrator user account is maintained in Enterprise Edge and access is closely controlled. Administrators must coordinate changes to avoid unintended changes.

Note: Do not use proxy servers while configuring Enterprise Edge using WEB OA&M. You must disable proxies and directly access Enterprise Edge. The configuration procedures depend on the browser and version.

Logging on to Enterprise Edge

To log on to Enterprise Edge:

1. Open a web browser.

2. In the URL address field, type the Enterprise Edge IP Address.
   For example: HTTP://10.10.10.1

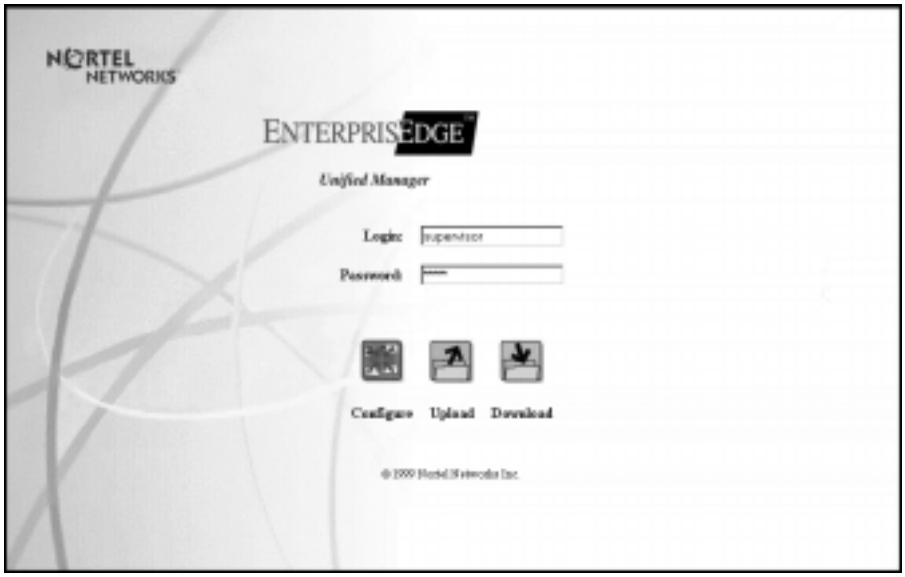
3. Press the **Enter** key.
   The Enterprise Edge log on screen appears.

4. In the **Login** box, type your login name.
   The default login name is *supervisor*.

5. In the **Password** box, type your password.
   The default password is *super*.

6. Click the **Configure** button.
   The Enterprise Edge Unified Manager software starts. Consult your system administrator for appropriate information. Depending on your system, Unified Manager software can take up to several minutes to initialize.

Enterprise Edge login screen



The login screen includes these boxes:

Field	Definition
Login	The user name. The name can contain up to 50 case-sensitive alphanumeric characters. The default log in name is s*upervisor*.
Password	The Enterprise Edge password. The password name can contain up to 12 case-sensitive alphanumeric characters. The default password is *super*.
Configure	lets you access Enterprise Edge configuration.
Upload	lets you upload and apply Enterprise Edge settings and system settings.
Download	lets you download and save Enterprise Edge settings and system settings.

Logging off Enterprise Edge

To log off Enterprise Edge:

1. Click the **Enterprise Edge** icon in the navigation tree.

2. On the menu click **Logoff** and then click **Logoff**.
   A message appears that asks you to confirm your request to log off.

3. Click the **Yes** button to log off.

Rebooting the Enterprise Edge server

To reboot the Enterprise Edge server:

1. Click **Logoff** and then click **Reboot**.
   A message appears that asks you to confirm your request to reboot.

2. Click the **Yes** button to reboot.

Configuring system settings

1. Click **Group** and then click **System** or **Comprehensive**.

2. On the navigation tree click the **Enterprise Edge** key and then click the **System** key.
   The screen displays the available Enterprise Edge item settings, resources and configurable resource services.

3. Configure item settings using Unified Manager and the resource services from the menu.
   Scroll to see any settings that do not appear.

NORTEL NETWORKS
ENTERPRISE EDGE
Group
Edit Configuration Performance Fault Report Tools Logoff View Help
Comprehensive
Add Delete Del All
Enterprise Edge
System
Resources
Services
Management
Base
System Name
EE_BETATA
[Format name]
Description
Resources
Name Status Version Description
LAN1 Up 3.4 10/100 Base T Ethernet NIC
WAN1 N/A 1.0 WAN Interface (T1/Upper Sy...
WAN2 Disabled 1.0 WAN Interface (Lower Sync) P...
Misc N/A 8.5.1 Enterprise Edge Media Servic...
Telephony
Services
Name Status Version Description
DHCP Disabled 4.1 Enterprise Edge DHCP Server
DNS Up 4.0 Enterprise Edge DNS Server i...
Routing Up 4.0 Enterprise Edge Multi Protocol...
SNMP Up 4.0 Enterprise Edge SNMP Agent
QoS Enabled 1.1 Enterprise Edge QoS Provider
VoIP Gateway N/A 8.5.1 Enterprise Edge VoIP Gateway
QoS Monitor Up 8.5.1 Voice Net Quality of Service ...
Web Cache Enabled 1.3.3 Apache Web Server in Cache...
Ready ...

The Unified Manager system settings are:

Setting	Definition
System Name	Lets users specify the system name of the Enterprise Edge Unified Manager.
Description	Shows a description of the Enterprise Edge Unified Manager installed system.
Resources	A configurable listing of all resources installed on the Enterprise Edge Unified Manager system.
Services	A configurable listing of services available for each resource on the Enterprise Edge Unified Manager system.

The resources and resource services are:

Column	Definition
Name	Shows each configurable resource service.
Status	Shows the status of each configurable resource service.
Version	Shows the version of each configurable resource service.
Description	Shows a brief description of each configurable resource service.

System name

Unified Manager often shows an example of how to format information to the right of the box. Type the information in that format.

To enter the system name:

1. In the **System Name** box type the system name.

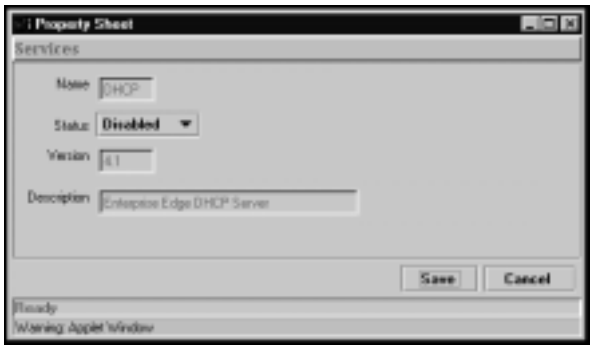
2. Press the **Tab** key to save your changes.

To configure system resources and services:

1. In the **Resource** options, click the resource you want to configure.

2. In the **Services** options, click the resource service you want to configure. Scroll to see any settings that do not appear.

3. On the menu click **Configuration** and then click **Modify Services**. The services dialog box appears.



4. From the **Status** list box enable or disable the resource service defined in the Name box.

5. Click the **Save** button to return to Unified Manager.

6. Repeat this process to enable or disable:

   •DHCP

   •DNS

   •Routing

   •SNMP

   •QoS

   •VoIP Gateway

   •Qos Monitor

   •Web Cache

   •Voice Record

   •TAPI Service Provider

   •Voice Service

   •Alarm Service

   •Voice Mail resource service

   •Msc

•Telephony resource

If a resource service is not highlighted prior to prompting resource modification, an error message appears that asks you to select a row in the table. Click the **OK** button to continue.

Note: For more information on configuring Enterprise Edge resources and services, refer to Configuring networking resources on page 63 and Configuring Enterprise Edge Services on page 185.

Status fields, where available, are the accumulation of 'administrative' and 'operational' status' of the component queried.

The three administrative statuses that can be assumed by a component are:

- **Enabled**: the component is enabled to operate in its normal mode, with all normal parameters set. When the component is enabled, the component can assume any of its operational statuses.
- **Disabled**: the component is disabled from operation. None of the component's operational statuses are valid in this state.
- **Paused**: the component is enabled and is running but is currently not accepting additional service requests.

The two operational statuses that can be assumed by a component are:

- **Up**: the component is up and running normally
- **Down**: the component is down, due to some reason - normal or abnormal, internal or external.

The Status column supports the combined list of these statuses:

- **Up**: This value is read-only. It indicates that the component is enabled and is operating normally. For a component like a network interface, this means the interface is enabled and connected to a valid link. For a service like DHCP, it means that the service is enabled and is running normally.
- When the current status is 'Up', setting it to 'Enabled' or 'Continue' where available, is a no-operation. Setting it to 'Disabled' disables the service, by shutting it down and then disabling it. Where available, setting it to 'Paused' pauses the service.
- **Down**: This value is read-only. This value indicates that the user has enabled the component, and the component is unable to operate in an 'Up' state because of normal or abnormal, internal or external errors. For example, if a network interface is not in an 'Up' state because of no connection to an actual physical link, it is a normal, external error. If a service like DHCP service is not in an 'Up' state because of internal errors, it is an abnormal, internal error.
- When the current status is 'Down' setting it to 'Enabled' attempts to bring it to 'Up' state again. As a result it may stay at a 'Down' state. Setting it to 'Disabled' disables the service. Where available, setting it to a 'Paused' or continued state fail as the service is not yet running.

- **Enabled**: This value is write-only. This value never appears when read. For a service that is enabled, one of its operational statuses (that is, Up or Down) appears when its Status field is read.
- When this value is set, it indicates that the user wants to enable the corresponding component and bring it to an 'Up' state. It is probable that the first happens. The second action depends on the component. For a network interface, the 'Up' state does not happen unless user connects a link to the interface. For a service this may not happen only if the system encounters an error of some kind during the requested action.
- **Disabled**: This value can be either read or set. When read, this indicates that the component is disabled from operation. When set, it indicates the same, in addition to taking the component to a 'Down' state before disabling.
- **Paused**: This value can be either read or set. When read, this indicates that the service is enabled and is given the command to pause. When set, it indicates the same, pausing the service further.
- **Continue**: This value can only be set. It can be set only when the service in a Paused state. It resumes paused service.

System name, date and time

To change the system name, date, and time:

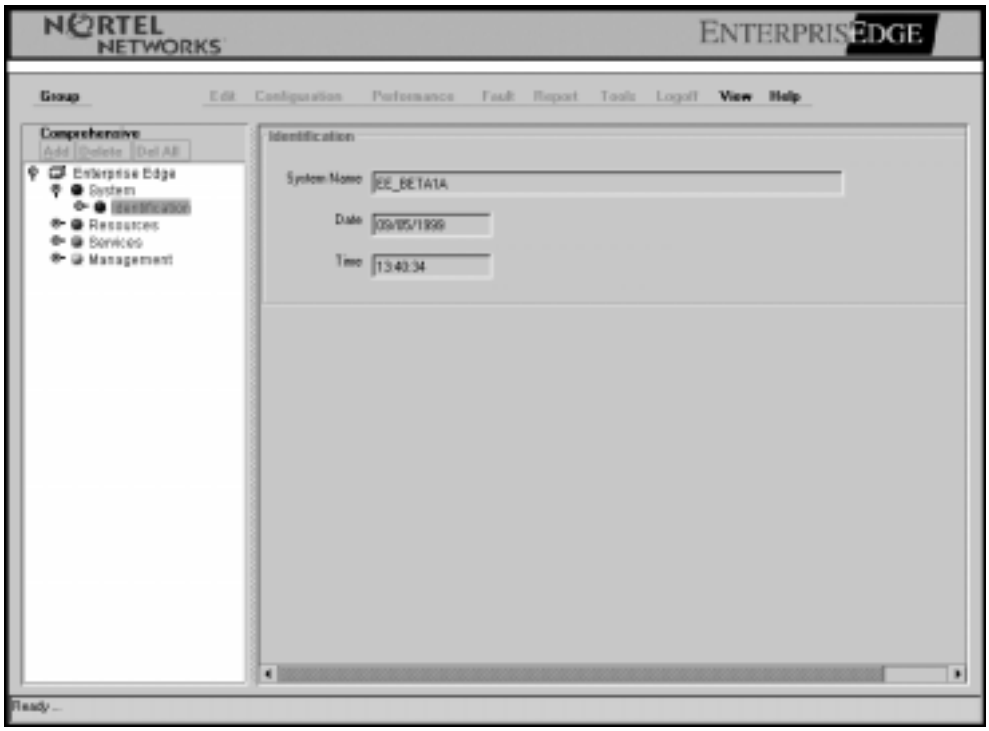
1. Click the **System** navigation key to expand the navigation tree.
   The System Settings dialog box appears.
   Clicking the System navigation key expands the navigation tree but doesn't display the summary of configurable Identification resources.

   The System Settings are:

Attribute	Description
Name	Lets users specify the name for the Enterprise Edge system. The Enterprise Edge system must have a unique name in the connected network (LAN or WAN) so that no two Enterprise Edge servers that can reach each other through IP network do not have the same name. The name must be less than 15 characters in length, cannot contain special characters like "/;," etc.
Date	Lets users set the current date for the Enterprise Edge system. Because the value for the date changes, save the changes as soon as the new date is entered.
Time	Lets users set the current time for the Enterprise Edge system. Because the value for the time keeps changing, save the changes as soon as the new time is entered. Use the 24-hour format to set the date. The seconds field is optional.

2. On the navigation tree click **Identification** to view the available system settings to configure.
   The System Identification dialog box appears.

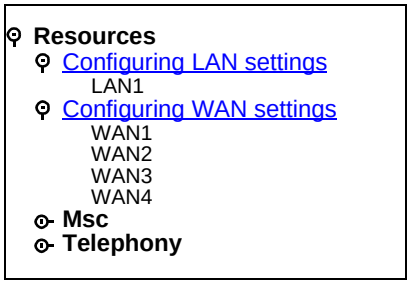
Note: Clicking the Identification navigation key causes the key to disappear. You must click Identification to display the configurable system settings.



3. In the **System Name** box type the system name.
4. In the **Date** box type the current date.
5. In the **Time** box type the current time.
6. Press the **Tab** key to save the changes.
7. Clicking the **System** navigation key to close the navigation tree.

Configuring networking resources 5

The following shows the programming map for networking resources:



Configure your networking resources using the information in:

- Viewing Enterprise Edge resources on page 63
- Configuring LAN settings on page 64
- Configuring WAN settings on page 66

Note: This chapter provides information on configuring LAN and WAN interfaces. For information on configuring MSC and Telephone, refer to Configuring Telephony Resources on page 77.

Viewing Enterprise Edge resources

To view the Unified Manager Resources screen:

1. On the menu click **Group** and then click **Resources** or **Comprehensive**.

2. On the navigation tree click **Enterprise Edge** and then click **Resources**. The available Enterprise Edge resources appear in table format. The table lists the name, operating status, software version, and description of each available resource:

Column	Definition
Name	The name column lists the available configurable resources.
Status	The status column lists the operating status of each configurable resource.
Version	The version column lists the software version of each configurable resource.
Description	The description column gives a brief description of the interface for each configurable resource.

3. Click the **Resources** navigation key to expand the navigation tree.

Configuring LAN settings

You configure LAN resource settings from Unified Manager.

If your Enterprise Edge server has more than one LAN interface, multiple items appear under LAN resources. To configure other LAN interfaces, follow the instructions given here for LAN1.

1. Choose **LAN** from the navigation tree to view the available LAN resources to configure. The available LAN interfaces (e.g., LAN1) appear in table format.

   Note: Clicking the LAN navigation key expands the navigation tree, but doesn't display the summary of configurable LAN resources.

2. Click the **LAN** navigation key to expand the navigation tree.

3. On the navigation tree click **LAN1**.
   Clicking the LAN1 navigation key causes the key to disappear. You must click **LAN1**.
   The LAN Summary screen for the LAN1 interface appears.

The following table lists and describes the attributes that the LAN Summary screen shows.

Attribute	Description
IP Address	Lets users specify the IP address of the LAN interface. Type the address in the following format: 255.255.255.255. The value for this field is valid only if the LAN interface is enabled.
SubNet Mask	Lets users specify the subnet mask of the LAN interface. Type the data in the following format: 255.255.255.255.
Physical Address	Lets users to view the physical address of the LAN interface. If the IP Address or subnet mask of the LAN interfaces changes, a DHCP scope associated with the LAN interface is created in the DHCP server running on the Enterprise Edge server. This scope contains all necessary parameters to the clients of the DHCP server configured so that they use Enterprise Edge as their default gateway and a WINS server. The scope also contains default parameters for the range of the addresses, based on the address of the Enterprise Edge interface and subnet mask. Navigate the services screen in the user interface to see DHCP settings for the scope.
Description	Lets users view a description of the network interface card supporting the LAN interface.
Version	Lets users view the version indicator of the LAN interface.
Speed	Lets users view the speed of the connection to the LAN interface. The value for this field is valid only if the LAN interface is enabled.

Attribute	Description
Connection Type	Lets users specify the connection type to the LAN interface. The following values are supported and are interpreted as follows: **Auto Sense**: The interface uses 'auto negotiation' protocol to choose the maximum possible speed of the connection. Depending upon the connected device, the interface can choose '100 MB' or '10MB', full-duplex or half-duplex. The receiving end's speed and connection type determines the mode of transmission. For example, if the receiving end is another PC port, or a bridge/switch port, the full duplex of operation is possible; if the receiving end is a shared media port (like hub port), only half-duplex mode is possible. **10 MB Half**: Speed is set to 10 MB/s and mode to half-duplex. **10 MB Full**: Speed is set to 10 MB/s and mode to full-duplex. **10 MB Auto**: The speed is set to 10 MB/s and the mode is automatically chosen by the interface, using auto-negotiation protocol. This mode is chosen to limit the maximum traffic coming into Enterprise Edge to 10 MB/s, while enabling the auto-negotiation feature for easier interconnection. Usually, you limit the incoming traffic if you notice that the bursty traffic from the connected LAN is degrading the quality of voice calls carried through VoIP over WAN. Though the LAN traffic gets lower priority in Enterprise Edge, their high rate of arrival to the Enterprise Edge server generates too may interrupts in the system that cause degraded quality in voice calls carried as VoIP. **100 MB Half**: Speed is set to 100 MB/s and mode to half-duplex. **100 MB Full**: Speed is set to 100 MB/s and mode to full-duplex.
Status	Lets users view the current status of the LAN interface. The possible states are: Up: the resource is operational. Down: the resource is not operational.

Consult your System Administrator for the appropriate configuration information before changing the settings.

To modify the configuration of the LAN1 settings:

1. In the **IP Address** box type the IP address.
   An example of how to format the information is shown at the right of the box.

2. In the **SubNet Mask** box type the subnet mask.

3. From the **Connection Type** list select the connection type.

4. Press the **Tab** key to save the settings.

To view LAN1 performance:

1. While at the LAN1 summary screen, on the menu, click **Performance** and then click **LAN Graph**.
   The LAN Graph: Statistic Chart appears.

2. On the menu, click **Performance** and then click **LAN Table**.
   The LAN Table: Statistic Table appears.

For information on using performance tables and graphs, refer to Graphs and tables on page 243.

3. Click the **LAN** navigation key to close the LAN portion of the navigation tree.

Configuring WAN settings

You configure WAN resource settings from Unified Manager.

WAN Interfaces have names such as WAN1 and WAN2. If your Enterprise Edge server has a permanent WAN card, WAN1 and WAN2 are interfaces from this card. These interfaces can run Frame Relay or PPP on a permanent WAN Link operating at T1 speed. Click on these interfaces to see their description.

If your Enterprise Edge server also contains a modem card with dial-up interfaces, these interfaces appear as WAN3, WAN4 and so on. Click on these interfaces to see their description. If your Enterprise Edge server does not have a WAN card, dial-up interfaces appear as WAN1, WAN2 and so on.

The configurable parameters and options are different for permanent WAN links and for dial-up WAN links. In this document, it is assumed that WAN1 and WAN2 are permanent WAN links and WAN3 and others are dial-up interfaces.

To view the WAN primary links:

1. Click **WAN** to view the available WAN resources to configure. The available WAN interfaces (e.g., WAN1) appear in table format.

   Note: Clicking the WAN navigation key expands the navigation tree, but doesn't display the summary of configurable WAN resources.

2. Click the **WAN** navigation key to expand the navigation tree.

3. On the navigation tree, click **WAN1** or **WAN2.**
   Clicking the WAN1 or WAN2 navigation key causes the key to disappear. You must click WAN1 or WAN2.
   The right frame displays the WAN Summary, WAN Line Parameters, WAN Frame Relay or PPP Parameters, and PVC Congestion Control screens.

   Note: The WAN Frame Relay Parameters do not appear unless frame relay is chosen as your link protocol in the WAN Summary. To display the WAN frame relay parameters, from the **Link Protocol** list box, select **Frame Relay**. Press the **Tab** key to update the screen. A configurable WAN PPP Parameters screen does not appear unless the current link protocol is PPP.

4. Scroll to view any settings that do not appear.

5. Configure the WAN Summary, WAN Line Parameters, WAN Frame Relay or PPP Parameters screens from Unified Manager. Configure the PVC congestion control screen using the menu. Refer to the following sections for details about the WAN Summary, WAN Line Parameters, WAN Frame Relay Parameters, WAN PPP Parameters, and PVC congestion control screens.

If your current link protocol is Frame Relay, you must configure WAN Frame Relay parameters and PVC Congestion Control entries. If your current link protocol is PPP, you must configure WAN PPP Parameters.

If the WAN port you are configuring is a T1 Port, you must configure WAN Line Parameters. If the port you are configuring is a synchronous (Sync) port, WAN Link Parameters have no effect, and are ignored. See the description of the port in WAN Summary section to see which port you are configuring.

WAN Primary Link Summary Parameters

To reach the WAN Summary screen, select **Resources, WAN,** then **WAN1** or **WAN2**. The WAN Summary screen attributes are:

Attribute	Description
IP Address	Lets users specify the IP address of the WAN interface. Type the data in the following format: 255.255.255.255.
SubNet Mask	Lets users specify the subnet mask in a valid dot format of the WAN interface. Type the data in the following dot format 255.255.255.255.
Physical Address	Shows the physical address of the WAN interface.
Description	Shows the description of the network interface card that supports the WAN interface.
Version	Shows the version indicator of the WAN interface.
Speed	Shows the operational speed of the WAN interface.

Attribute	Description
Status	Shows the current resource status of the WAN interface. The possible states are: Up: the resource is operational. Down: the resource is not operational.
Link Protocol	Lets users specify PPP or frame relay protocol. If you change the link protocol, the configuration screen changes to include fields corresponding to the link protocol you choose. To ensure proper operation, always refresh the page by clicking **View** and then **Refresh**.
Compression	Lets users enable or disable data compression.
Frame Size	Lets users specify the maximum frame size for the layer-2 packet carried on this port.

To modify the configuration of the WAN1 or WAN2 summary screen:

1. In the **IP Address** box type the IP address.
2. In the **SubNet Mask** box type the subnet mask.
3. From the **Link Protocol** list box choose **Frame Relay** or **PPP**.

   Note: If you choose Frame Relay, press the **Tab** key to update the screen. A configurable WAN Frame Relay Parameters screen appears.

4. From the **Compression** list box select to enable or disable compression.
5. In the **Frame Size** box type the frame size.
6. Press the **TAB** key to save your settings.

WAN Primary Link Line Parameters

Scroll down from the WAN Summary screen to find the WAN Line Parameters screen. The WAN Line Parameters attributes are:

Attribute	Description
Channel Rate	Lets users set the data rate for each of the DS0 channels in the T1 line.
Clock Source	Lets users set an internal or external T1 clock source.
Frame Type	Lets users set the type of framing to be adopted in the T1 line. You can select either SF(D4) or ESF for the frame type. SF(D4) transmits superframes consisting of 12 individual frames. ESF transmits superframes consisting of 24 individual D4 frames and provides enhanced signaling and synchronization. ESF lets you test the digital line while it is in use. Always use the frame type that the equipment at the receiving end expects.

Attribute	Description
Line Coding	Lets users set the type of encoding used in the T1 line. You can select either B8ZS or AMI for this parameter. B8ZS (Bipolar with 8 Zero Substitution) line coding replaces a block of eight consecutive binary zeros with an 8-bit B8ZS code containing bipolar violations in the fourth and seventh bit positions of the substituted code. In the receiving direction, the B8ZS code is detected and replaced with eight consecutive binary zeros. AMI line coding is also bipolar: a binary zero is transmitted as zero volts, and a binary 1 is transmitted as either a positive or negative pulse, opposite in polarity to the previous pulse. Always use the line coding method that the equipment at the receiving end expects.
Line Polarity	Lets users set normal or inverted line polarity in the T1 line. The option inverted is meaningful only if LineCoding is AMI.
Pulse Density	Lets users control whether the DSU/CSU maintains the minimum level of 1s on the line for AMI encoding.
Channel List	Lets users create a list of channels used in the T1 line. You can specify multiple channel numbers in a comma-separated list. Each item in the list can contain a range of channel numbers, with the limits of the range separated by a hyphen. For example, a valid entry for channel list is 3,5,6,10-15,18,20-23. Specify the use of all the channels by using the string "All".

To modify the configuration of the WAN1 or WAN2 Line Parameters screen:

1. From the **Channel Rate** list box select the channel rate.
2. From the **Clock Source** list box select the clock source.
3. From the **Frame Type** list box select the frame type.
4. From the **Line Coding** list box select the line coding.
5. From the **Line Polarity** list box select the line polarity.
6. From the **Pulse Density** list box select the appropriate pulse density and close the list box.
7. In the **Channel List** box.type the channel list.
   Specify a list of channels numbers or their ranges separated by a comma or hyphen. Ranges can be mixed with individual entries.
8. Press the **Tab** key to save the settings.

WAN Primary Link Frame Relay Parameters

If you chose Frame Relay as your link protocol, scroll down from the WAN Line Parameters screen to find the WAN Frame Relay Parameters screen. The WAN Frame Relay Parameters are:.

Attribute	Description
LMI Type	Lets users set the type of link management protocol used on this link. This type must match the corresponding type set in the Frame Relay service provider's switch. Permitted types are ANSI, LMI, and CCITT. The default setting is ANSI.
Polling Interval	Lets users set an interval, in seconds, between LMI status inquiry messages. This value must match the corresponding value set in the Frame Relay provider's switch. Permitted values are between 5-30 seconds. The default setting is 10.
Full Enquiry Interval	Lets users set the maximum number of LMI Status Enquiry messages sent before sending a Full Status Enquiry request. This value must match the corresponding value set in the Frame Relay provider's switch. Permitted values are between 1 and 255 (in seconds). The default setting is 6.
Error Threshold	Lets users set the maximum number of consecutive failures permitted in LMI Status Enquiry before marking the link non-operational. It is also the number of successful consecutive LMI Status Enquiry messages that must be received before marking a link as operational. Permitted values are between 0 and MAXINT. The default setting is 3.
Monitored Events	Lets users set the number of events sampled for making decisions about the error threshold. Set the number higher than the values set in the error threshold. Permitted values are a number between 0 and MAXINT. The default setting is 4.
DS Code	Lets users set the differentiated services code (DSCode) recognized by the frame relay driver for prioritization. This value is used as a mask value. When an IP packet is sent down, the frame-relay driver checks whether the packet's DSCode field (known as TOS byte in earlier documents) has any of the bits specified in this field set (a bitwise AND operation is performed between this field's value and the DSCode field of the IP packet and the result is checked for 0). If any of the bits is set (result is non-zero), the frame relay network is signaled to handle this packet with priority by clearing the 'D/E' (discard eligibility) bit in the frame relay packet header. If none of the bits specified in this field are set in the IP packet header, 'D/E' bit is set in the frame-relay packet header, marking the packet as a likely candidate for packet drop in case of congestion in the frame relay network. This field's value carries the same semantics as the 'differentiated services codepoint' discussed in RFC2474. The least significant two bits are ignored.
Compression Enabled PVCs	Lists PVCs on which compression is enabled. If the compression field is Disabled, the field does not have any meaning. If the compression field is Enabled, compression and decompression are performed on the data going to and coming from the PVCs in this list. The value can be a comma-separated list of DLCI numbers. You can specify a range of DLCIs by specifying the lower and upper boundaries by a hyphen. You can mix individual numbers and ranges.

Attribute	Description
Access Rate	Lets users set, in kbps, the maximum access rate on the interface running frame-relay. The frame-relay congestion control engine uses this value to limit or shape traffic. Specify a value computed using the T1 channels available for data communication on the port attached to this interface and their data rates.

To modify the configuration of the WAN Frame Relay Parameters:

1. From the **LMI Type** list box select the LMI type.
2. In the **Polling Interval** box type the polling interval in seconds.
3. In the **Full Enquiry Interval** box type the full enquiry interval.
4. In the **Error Threshold** box type the error threshold.
5. In the **Monitored Events** box type the appropriate monitored events.
6. In the **DS Code** box type the DS code.
7. In the **Compression Enabled PVCs** box type the compression enabled PVCs list.
8. In the **Access Rate** box type the access rate in kbps.
9. Press the **Tab** key to save the settings.

Scroll down from the WAN Frame Relay Parameters screen to find the PVC Congestion Control table. The WAN PVC Congestion Control settings are:

Column	Description
Entry (CC#)	Uniquely identifies the congestion control entry on the interface. Use the format specified for the entry identifier. It must include the prefix 'CC' followed by a unique number in the table. For example, 'CC2' is a valid number. If you don't use consecutive numbers while adding the entry, the system adjusts them to be consecutive. If you specify an existing entry while adding an entry, the existing entry is modified with new values. While modifying an entry, the name can't be changed.
DLCI	Lets users set the DLCI number for the PVC to be congestion controlled. If a DLCI is not configured, it is not congestion controlled. Enterprise Edge uses one-second intervals to measure this parameter.
CIR	Lets users set, in kbits, the carrier guarantees the router transmits over a specified time interval when congestion is not present. Enterprise Edge uses one-second intervals to measure this parameter.
Committed Burst (bC)	Lets users to define the number, in kbits, of bits the router transmits over a specified time interval if congestion is present. Usually this value is set for 1/4 the value of the CIR. Enterprise Edge uses one-second intervals to measure this parameter.

Column	Description
Excess Burst (Be)	Combined with the committed burst rate, lets users set, in kbits, the maximum number of bits the router transmits over a specified time interval if there is no congestion. Both Be and bC must be less than or equal to the line speed.

To add PVC congestion control:

1. On the menu click **Configuration** and then click **Add PVC Congestion Control**.
   The PVC Congestion Control dialog box appears. If an entry range has not been selected an error message appears.

2. In the **Entry (CC#)** box type the entry “CCxx” where “xx” is a unique integer.

3. In the **DLCI** box type the DLCI.

4. In the **CIR (kbps)** box type the CIR in kbps.

5. In the **Committed Burst BC (kbits)** box type the committed burst in kbits.

6. In the **Excess Burst BE (kbits)** box type the excess burst in kbits.

7. Click the **Save** button to save the entries and return to Unified Manager.

To modify PVC congestion control:

1. Click an entry in the PVC Congestion Control range.

2. On the menu click **Configuration** and then click **Modify PVC Congestion Control**.
   The PVC Congestion Control dialog box appears.

3. Click any box that requires modification and type the necessary changes.

4. Click the **Save** button to save the modifications and return to Unified Manager.

To delete PVC congestion control:

1. Click an entry in the PVC Congestion Control range.

2. On the menu click **Configuration** and then click **Delete PVC Congestion Control**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to delete PVC congestion and return to Unified Manager.

WAN Primary Link PPP parameters

If you chose PPP as your link protocol, scroll down from the WAN Line Parameters screen to find the WAN PPP Parameters screen. The WAN PPP Parameters are:

Attribute	Description
Keep Alive Interval	Lets users specify the interval between kept alive messages sent when there is no regular traffic on the PPP link.
Cisco's Encapsulation Mode	Lets users enable or disable the Cisco compatibility mode.

To set the WAN PPP parameters:

1. In the **Keep Alive Interval** box, type the keep alive interval in seconds.

2. From the **Cisco's Encapsulation Mode** list box, enable or disable the Cisco compatibility mode.

WAN Primary Link performance graphs and tables

To access the WAN Primary Link performance graphs and tables:

1. On the menu click **Performance** and then click **WAN Graph**.
   The WAN Graph: Statistic Chart appears.

2. On the menu click **Performance** and then click **WAN Table**.
   The WAN Table: Statistic Table appears.

For information on using the WAN statistic chart and the WAN statistic table, refer to Graphs and tables on page 243.

WAN Backup Links

WAN3 and WAN4 are dial-up interfaces that are configured according to the V.90 modem in the Enterprise Edge server. You must click WAN3 to see its description.

Dial-up WAN Links always use PPP as the link-layer protocol. For proper operation, the links must be connected to PPP-capable RAS Servers that can run RIP or can accept static routes.

To view the WAN backup link parameters:

1. On the navigation tree, click **WAN3**.
   The WAN Summary, WAN Link Parameters, and WAN Access Parameters screens appear.

   Note: Clicking the WAN3 navigation key causes the key to disappear. You must click **WAN3**.

2. Scroll to see any settings that are not displayed.

WAN Backup Summary Parameters

The WAN Summary contains these settings:

Setting	Definition
IP Address	Lets users set the IP address of the modem interface when it connects. Users can set a fixed IP Address for the dial-up interface. If a fixed address is specified, it is used by Enterprise Edge to connect to the receiving end. Alternatively, users can choose RemoteAssigned to indicate that Enterprise Edge must obtain an IP address from the remote end and use it. The address obtained depends on the RAS server that the Enterprise Edge server connects to.
Description	Shows a description for the subsystem that is encapsulated by the DLL.
Version	Shows the version for the subsystem that is encapsulated by the DLL.
Status	Lets users set the modem interface resource status. The possible states are: Up: the auto WAN backup service is enabled and the dial-up link is currently connected. Down: the auto WAN backup service is enabled and the dial-up link is currently disconnected. Enabled: the interface is enabled for use by the auto-backup server. Disabled: the auto WAN backup service is disabled.

To set the WAN Summary attributes for the WAN backup link:

1. From the **IP Address** list box select the appropriate IP address assignment or type a new value.

2. From the **Status** list box enable or disable the connection to the backup link.

3. Press the **Tab** key to save the settings.

WAN Backup Link Parameters

Scroll down from the WAN Summary screen to find the WAN Link Parameters screen. The WAN Link Parameters are:

Attribute	Description
Telephone Number	Lets users specify a telephone number to be used to connect using the modem interface. If needed, include area codes, if any, and all necessary digits to dial an external number.
Alternate Telephone Number	Lets users specify an alternate number to be used to connect using the modem interface. Include area codes, if any, and all necessary digits to dial an external number.
Connect Rate	Lets users specify the initial speed (in bits per second) for the modem to connect. Set to the maximum permissible value for best results. Permitted values: 57600, 38400, 19200, 9600, 4800. Note: This is the initial rate, actual rate is always negotiated.

Attribute	Description
Dial Retries	Lets users specify the number of tries the system attempts to make a link operational before marking it non-operational. A positive number must be used.
Dial Interval	Lets users specify the interval, in seconds, between successive attempts to make a link operational.
Speaker Mode	Lets users enable or disable the speaker during initial link establishment.
IP Header Compression	Lets users enable or disable IP header compression. To function, the receiving end must utilize this feature to work.
Software Compression	Lets users enable or disable data compression in the software, instead of the modem. For dial-up connections, Unified Manager uses Microstate Point-to-Point Compression algorithm (MPPC).
Hardware Compression	Lets users enable or disable data compression in the hardware instead of the software.
PPP LCP Extensions	Lets users specify whether or not to enable or disable PPP LCP extensions that include Time-Remaining, Identification, and Callback features. The Callback feature is not supported even if LCP extension is enabled.

To set the link parameters for the WAN backup link:

1. In the **Telephone #** box type your telephone number choice.
2. In the **Alternate Telephone #** box type your alternate telephone number choice.
3. From the **Connect Rate** list box select your connection rate choice.
4. In the **Dial Retries** box type the number of times to attempt dialing if the connection fails.
5. From the **Speaker Mode** list box select your speaker mode choice.
6. From the **IP Header Compression** list box select enable or disable.
7. From the **Software Compression** list box select enable or disable.
8. From the **Hardware Compression** list box select enable or disable.
9. From the **PPP LCP Extensions** list box select enable or disable.
10. Press the **Tab** key save the settings.

WAN Backup Access Parameters

Scroll down from the WAN Link Parameters screen to find the WAN Access Parameters screen. The WAN Access Parameters are:

Attribute	Description
Authentication	Lets users specify the authentication type for the link. Users can choose AllowClearText or EncryptedOnly. If EncryptedOnly is selected, only encrypted authentication such as CHAP is used on this interface during PPP authentication protocol. If AllowClearText is selected, CHAP is used first and if the receiving end of the link declines, PAP is used to authenticate the link user.
Two Way Authentication	Lets users enable or disable link authentication in both directions.
User ID (name password)	Lets users specify a user name and a password that the link uses to authenticate itself while dialing out to another router.

To set the access parameters for the WAN backup link:

1. Scroll to find the WAN Access Parameters.
2. From the **Authentication** list box select the authentication type.
3. From the **Two Way Authentication** list box select the two-way authentication type.
4. In the **User ID (name password)** box type the user ID, separating the user name and password with a space.
5. Press the **Tab** key to save the settings.
6. Click the **WAN** navigation key to close the navigation tree.

Configuring Telephony Resources 6

The Telephony heading allows you to program and manage all the voice components associated with Enterprise Edge. It includes information such as how to set up lines and trunks, define settings for individual telephones, how to customize your telephone network to suit your requirements, and so on. From the Unified Manager, expand **Resources** and **Telephony** to view the Telephony subheadings.

The Telephony subheadings are briefly summarized in the table below. Note that the Maintenance and Metrics headings are described in Maintenance on page 233.

Note: To jump to any section for more information, click the blue, underlined text and the information is automatically displayed.

Terminals &Sets	Allows you to assign settings to each telephone.
Lines	Allows you to assign settings to each trunk and target line.
Restriction filters	Allows you to apply restriction filters for external calls
Services	Allows you to create services such as night ringing, routing and restrictions for making external calls.
System speed dial	Allows you to create speed dial codes that can be used by any telephone in the system.
Passwords	Allows you to view and change passwords.
Time and date	Allows you to set the time and date on the system clock.
General settings	Allows you to change system-wide settings.
Hunt groups	Allows you to create and manage hunt groups
Companion	Allows you to assign settings for portable telephones
Telco features	Allows you to assign settings for external voice message services.
Software keys	Allows you to access system identification and enter software keys when adding features to the system.
Hardware	Allows you to configure the trunks and modules used by the system.
Maintenance	Allows you to perform routine system maintenance such as backup and restore and allows you to provision modules.
Metrics	Allows you to see diagnostic information about the system.

By selecting **Telephony**, the **Tools** menu is enabled, which allows you access to the Backup and Restore tool. For more information on using the Backup and Restore tool, refer to Backup and restore on page 234.

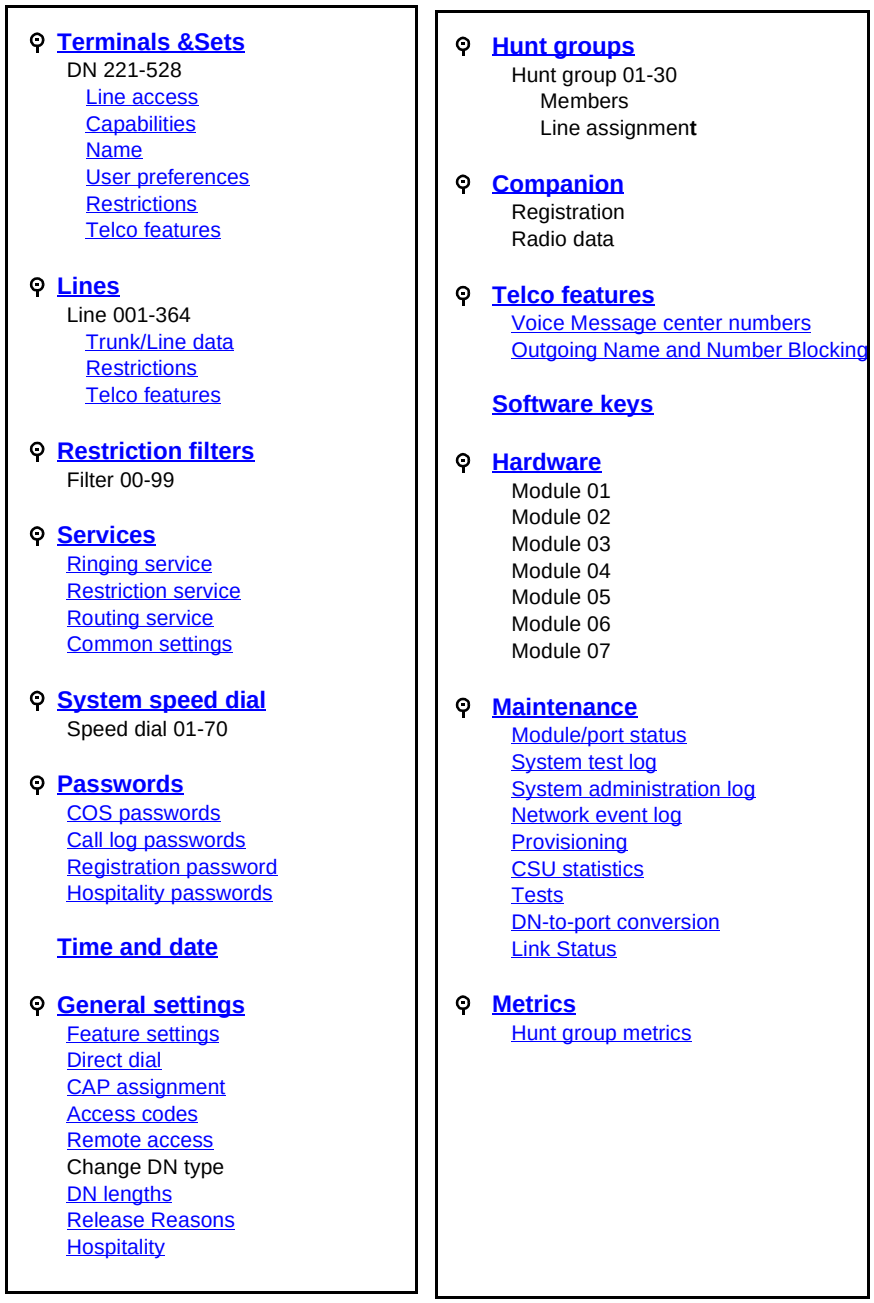
Programming order

The following programming order is recommended when you initially start programming your Enterprise Edge system:

1. Hardware
2. Software keys
3. Lines
4. Terminals & Sets
5. General settings
6. Services
7. Companion and Hunt groups
8. System speed dial and Telco features
9. Passwords
10. Time & date

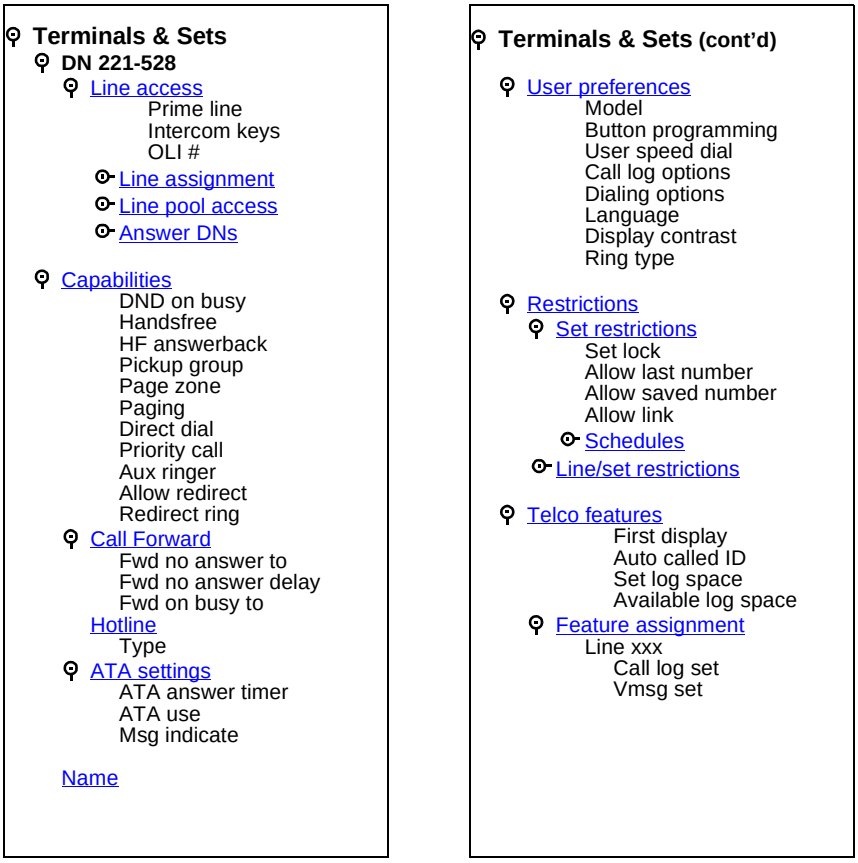
Programming affects system operation.
Only a qualified person should perform startup, installation and maintenance programming. Many of the settings affect the correct operation of the system.

The following illustration shows an overview of the Enterprise Edge programming that is accessible through the Unified Manager.


Terminals &Sets
DN 221-528
Line access
Capabilities
Name
User preferences
Restrictions
Telco features
Lines
Line 001-364
Trunk/Line data
Restrictions
Telco features
Restriction filters
Filter 00-99
Services
Ringing service
Restriction service
Routing service
Common settings
System speed dial
Speed dial 01-70
Passwords
COS passwords
Call log passwords
Registration password
Hospitality passwords
Time and date
General settings
Feature settings
Direct dial
CAP assignment
Access codes
Remote access
Change DN type
DN lengths
Release Reasons
Hospitality
Hunt groups
Hunt group 01-30
Members
Line assignment
Companion
Registration
Radio data
Telco features
Voice Message center numbers
Outgoing Name and Number Blocking
Software keys
Hardware
Module 01
Module 02
Module 03
Module 04
Module 05
Module 06
Module 07
Maintenance
Module/port status
System test log
System administration log
Network event log
Provisioning
CSU statistics
Tests
DN-to-port conversion
Link Status
Metrics
Hunt group metrics

Terminals &Sets

The Terminals & Sets heading allows you to assign settings to each telephone. The following illustration shows a detailed view of the Terminals & Sets programming map.



Copying settings from one telephone set to another

The Copy command allows you to duplicate programming for a telephone and apply it to another telephone, a range of telephones or all the telephones on the system.

To copy settings from one telephone to another:

1. Choose **Resources, Telephony, Terminals & Sets**.
2. Click the telephone set (DN 221-528) from which you want to copy settings.
3. If necessary, choose a subheading to refine your selection.
4. On the **Edit** menu, click **Copy**.
5. Click **Single** from the Copy type list box.

6. Type the DN number of the set to which you want to copy the settings.

7. Click the **OK** button.

To copy programming from one telephone to a range of telephones:

1. Choose **Resources, Telephony, Terminals & Sets**.

2. Click the telephone set (DN 221-528) from which you want to copy settings.

3. If necessary, choose a subheading to refine your selection.

4. On the **Edit** menu, click **Copy**.

5. Click **Range** from the Copy type list box.

6. Type the start and end DN numbers of the sets to which you want to copy the settings.

7. Click the **OK** button.

To copy programming from one telephone to all telephones:

1. Choose **Resources, Telephony, Terminals & Sets**.

2. Click the telephone set (DN 221-528) from which you want to copy settings.

3. If necessary, choose a subheading to refine your selection.

4. On the **Edit** menu, click **Copy**.

5. Click **All** from the Copy type list box.

6. Click the **OK** button.

Line access

Line access allows you to assign lines to individual telephones. To save time, you can copy the Line access settings to other telephones once you have finished programming the settings for one telephone.

Note: PRI lines must be set to Auto Answer and cannot be Manual Answer.

To assign a line to a telephone:

1. Choose **Resources**, **Terminals & Sets**, **Line access**.

2. Configure line access according to the table:

Attribute	Description
Prime line	Defines the first line that is selected when a call is made from an Enterprise Edge telephone. Values: None, Pool (A to O), I/C (intercom), or Line: (Default: None)
Intercom keys	Assigns the number of intercom buttons to a telephone. Intercom buttons provide a telephone with access to internal and external lines, and line pools. Values: 0 to 8
OLI #	Defines the digits used for originating line identification number (OLI). Values: up to 24 digits (Default: blank)

Prime line

This setting assigns a prime line to the telephone. A prime line is the first line that is automatically selected when a call is made from an Enterprise Edge telephone. Only assigned lines and line pools appear. PRI pools are not valid selections for a Prime line.

An assigned prime line is not associated with the assignment of a prime telephone.

An external line must be assigned to the telephone in Line assignment before it can be assigned as the prime line to the telephone. A line pool must be assigned to the telephone in line pool access before a line pool can be assigned as the prime line to the telephone. A target line cannot be a prime line for a telephone because it is incoming-only.

A T1 DID line should not be assigned as the prime line for a telephone. If assigned, it is treated as if no prime line has been assigned. The message **Select a line** appears when the receiver is lifted.

By assigning a line pool as a prime line, a telephone can be made to search automatically for an idle line in a pool. For more information, see Line type on page 101.

Intercom keys

This attribute assigns the number of intercom buttons to a telephone, which provide a telephone with access to internal and external lines, and line pools.

Each intercom button assigned during programming automatically appears on the telephone. The buttons start with the lower right-hand button, or one button above if the Handsfree/Mute feature is assigned to the telephone.

The following should be noted when assigning the number of Intercom keys:

- A telephone requires two intercom buttons to be able to establish a conference call with two other Enterprise Edge telephones.
- Only one intercom button may be required if the button is only used to make and receive internal calls, and to access line pools. Two intercom buttons are required if a telephone has several lines assigned to ring only.
- The M7100 telephone can be assigned up to eight intercom buttons even though the telephone has only one programmable button.

OLI

Enter the digits used for the originating line identification number (OLI).

Line assignment

This setting allows you to assign physical trunks and target lines to each telephone. Target lines are assigned and removed in the same manner as other lines.

Broadcast ring group ability is possible with multiple target line assignment across a group of sets.

To assign a trunk or target line to a telephone:

1. Choose **Resources**, **Telephony**, **Terminals & Sets**.
2. Click the telephone set (DN 221-528) to which you want to assign a trunk or line.
3. Choose **Line access**, **Line assignment**.
4. Click the **Add** button.
5. Type a line number in the Line box.
6. Click the **Save** button.
7. Click one of the following to define the line appearance type: **Unassigned**, **Ring only**, **Appear&Ring**, or **Appear only**.

Appearances

The Enterprise Edge system can handle simultaneous calls to the same DID line on the same set (multiple target line appearances). The number of DID appearances depends on the **Appearance type** setting (**Appear&Ring**, **Ring only**, **Appear only**).

Note: This setting only applies for direct inward dial (DID) lines 241-336. These lines are also referred to as target lines.

Select the line number you want, the **Appearance type** setting, and for **Appearances**, enter the number of target line appearances.

The Enterprise Edge system will not support a mixture of **Appear only** and **Ring only** appearances for the same line.

If **Appear&Ring** or **Appear only** is chosen, you can have as many simultaneous DID calls as there are target line key appearances. If **Ring only** is chosen, you can have as many simultaneous DID calls as you have intercom keys.

PRI Lines

Users cannot access PRI lines directly through line appearances or line pools. All outgoing PRI calls are dialed using the intercom button and entering a routing code.

When an EE-DTM is changed to PRI, all existing line appearances for that module are automatically removed.

The Enterprise Edge Analog Terminal Adapter (ATA 2), or a portable cannot process more than 2 simultaneous calls.

There is a suggested limit of 4 keys per set. You can program more than 4 keys on a set by programming less than 4 on other sets. For instance, you might program 20 keys on a receptionist set equipped with a CAP.

Tips

In general, auto-answer loop start trunks, auto-answer T1 E&M trunks and T1 DID trunks are not assigned to telephones. If assigned, they are used for monitoring incoming call usage, or for making outgoing calls (auto-answer loop start and T1 E&M trunks).

You cannot assign a line that is private to another telephone.

Each line assigned to appear at a telephone must appear at a button with an indicator on that telephone. The maximum number of line buttons are 8 for the M7208 telephone, 10 for the M7310 telephone, and 24 for the M7324 telephone.

If you set a line to Ring only, incoming calls appear on an intercom button.

A central answering position (CAP), with one or two CAP modules, can provide extra line buttons if more than 24 lines are assigned to the CAP. The remaining lines appear at buttons on the CAP module.

The M7100 telephone is an exception; it has no line buttons and can be assigned any number of lines.

Make sure that lines assigned to an M7100 telephone are assigned to ring; otherwise, you cannot detect incoming calls on the lines.

Line pool access

This setting allows a telephone to access one or more of the fifteen line pools available (A to O). Six exclusive line pools (PRI-A to PRI-F) are available for PRI lines. Only three are currently supported.

Only PRI lines can belong to a PRI pool. PRI lines cannot belong to Line Pools A through O, and all lines on a single EE-DTM (PRI) belong to the same pool. Lines from multiple EE-DTM (PRI) can belong to the same pool if they are configured with the same protocol. PRI lines are assigned to pools with the **Line type** setting.

To assign a telephone to a line pool:

1. Choose **Resources**, **Telephony**, **Terminals & Sets**.
2. Click the telephone set (DN 221-528).
3. Choose **Line access**, **Line pool access.**
4. Click the **Add** button.
5. Enter a letter from **A** to **O**.
6. Click the **Save** button.

   The set can now access any lines in that line pool.

Answer DNs

Calls for other Enterprise Edge telephones can appear and be answered at the telephone being programmed. The DNs of the other telephones are referred to as Answer DNs.

Every Answer DN assigned to the telephone automatically assigns an Answer button with an indicator to the telephone. These buttons should be labeled accordingly, identifying the telephone with its name or DN.

The maximum number of Answer DNs that can be assigned to a particular Enterprise Edge set is eight.

Every Answer DN assigned to the telephone automatically assigns an Answer button with an indicator to the telephone. These buttons should be labeled accordingly, identifying the telephone with its name or DN.

The maximum number of Answer DNs that can be assigned to a particular Enterprise Edge set is eight.

More than one telephone can have an Answer button for the same DN. In this way, more than one telephone can provide call alerting and call answering for any calls directed to that DN.

To create an answer DN:

1. Choose **Resources**, **Telephony**, **Terminals & Sets**.
2. Click the telephone set (DN 221-528).

3. Choose **Line access**, **Answer DNs.**
4. Click the **Add** button.
5. Type the Answer DN.
6. Click the **Save** button.
7. Click one of the following to define the Answer type: **Unassigned**, **Ring only**, **Appear&Ring**, or **Appear only**.

Capabilities

Settings that control how the system interacts with individual telephones and the calls they receive are found in Capabilities.

To define telephone capabilities:

1. Choose **Resources**, **Telephony**, **Terminals & Sets**.
2. Click the telephone set (DN 221-528).
3. Choose **Capabilities.**
4. Configure Capabilities according to the table:

Attribute	Description
DND on busy	Defines whether an incoming call rings if the user is already on another call. Values: Y or N (Default: N)
Handsfree	Defines whether Handsfree will be available to a telephone. Values: Auto, Standard, None (Default: None)
HF answerback	Defines whether a user can automatically answer a voice call without lifting the receiver or pressing the Handsfree/Mute button. Values: Y or N (Default: Y)
Pickup group	Assigns a telephone to a pickup group. Values: None, 1 to 9 (Default: None)
Page zone	Assign a telephone to page zone. Values: None, 1 to 6 (Default: 1)
Paging	Defines whether paging announcements can be made from a telephone. Values: Y or N (Default: Y)
Direct dial	Defines whether you can call the Direct-dial telephone from this telephone using the Direct-dial digit. Values: Set 1 to Set 5, None (Default: 1)

Attribute	Description
Priority call	Select whether to allow this telephone to interrupt calls or to override Do Not Disturb at another telephone. Values: Y or N (Default: N)
Aux ringer	Defines whether an auxiliary ringer (if installed) will ring for incoming calls at this telephone. Values: Y or N (Default: N)
Allow redirect	Defines whether or not to allow this telephone to redirect its lines. Values: Y or N (Default: N)
Redirect ring	Select whether a telephone rings briefly when a call on one of its lines is redirected by the Line Redirection feature (Feature 8 4). Values: Y or N (Default: Y)

Call Forward

The Call Forward heading allows you to define how calls are handled when they are unanswered or the line is busy.

To program call forward:

1. Choose **Resources**, **Telephony**, **Terminals & Sets**.
2. Click the telephone set (DN 221-528).
3. Choose **Capabilities, Call Forward.**
4. Configure Call Forward according to the table:

Attribute	Description
Fwd no answer to	Redirect all incoming calls when this telephone does not answer. Values: up to 24 digits (Default: blank)
Fwd no answer delay [1]	Defines the number of rings before an unanswered call is forwarded. Values: 2, 3, 4, 6, 10 (Default: 4)
Fwd on busy to	Redirects all incoming calls when this telephone is busy with another call. Values: up to 24 digits (Default: blank)
Notes: 1 Appears after you have typed in a call forward no answer number and press Enter.	

Hotline

The Hotline heading allows you to define a telephone number that will be dialed automatically when a user lifts the receiver or presses the Handsfree/Mute button.

To define an internal number as a hotline:

1. Choose **Resources**, **Telephony**, **Terminals & Sets**.

2. Click the telephone set (DN 221-528).
3. Choose **Capabilities, Hotline**
4. Click **Internal** and press Enter.
5. In the **Internal #** box, type the DN number (up to 3 digits).

To define an external number as a hotline:

1. Choose **Resources**, **Telephony**, **Terminals & Sets**.
2. Click the telephone set (DN 221-528).
3. Choose **Capabilities, Hotline**
4. Click **External**.
5. In the **External #** box, type the telephone number (up to 24 digits).
6. Click a Facility value: **Use prime line**, **Use line:**, **Pool code:**, **Use routing table**.

   Note: For Pool type a letter from A to O and press Enter. For Use line type a number from 001 to 238. and press Enter. Target lines cannot be used as the facility.

ATA settings

The ATA settings heading allows you to define general settings for analog terminal adapters.

To configure ATA settings:

1. Choose **Resources**, **Telephony**, **Terminals & Sets**.
2. Click the telephone set (DN 221-528).
3. Choose **Capabilities, ATA Settings.**

4. Configure ATA Settings according to the table

Attribute	Description
ATA answer timer	Select the length of delay between the last digit you dial and when the Enterprise Edge ATA 2 device is ready to receive DTMF tone. Values: 3, 5, 7, 10 (Default: 7)
ATA use	Select where the Enterprise Edge ATA 2 can be used. Values: On site, Off site (Default: Off site)
Msge Indicate	Select the type of message indicator. Tone sends a Message Tone through the set's receiver and Lamp turns on the set's Message Lamp when a message is received. Values: None, Tone, Lamp (Default: None)

Enterprise Edge Analog Terminal Adapter settings (ATA 2)

The analog terminal adapter converts digital interface signals to analog for communication with analog devices such as single line telephones, fax machines, and modems.

ATA answer timer

A timer can be used to administer a delay between the last digit you dial on a device connected to Enterprise Edge ATA 2 and when the system begins to send out tones (DTMF or modem) on the outgoing line without capturing and interpreting them.

Tip

If a modem or fax machine is attached, you will want to keep the delay short. If a call to a fax machine or modem cannot be connected, try shortening the delay. If an individual is dialing the number for a fax machine or modem, you may want to make the delay a little longer.

ATA use

Enterprise Edge ATA 2 can connect to devices that are either on your premises or at some other location. Select On site or Off site.

Msge Indicate

Select the type of message indicator to be activated when a set receives a message. Select None, Tone, or Lamp.

Name

The default name for a telephone is its DN but the name can be changed to a more descriptive name if desired.

To assign a name to a telephone:

1. Choose **Resources**, **Telephony**, **Terminals & Sets**.
2. Click the telephone set (DN 221-528).
3. Click **Name.**
4. Type a name up to seven characters and press Enter.

   Note: The name may be a combination of letters and numbers.

User preferences

Any programming that can be done by users at their telephones can also be done in the Unified Manager. The default settings are given in bold. If the attached set is not an Enterprise Edge set, these options are not available.

Setting	Description
Model	Allows you to pre-program the model of Enterprise Edge set which will use this DN (M7310). The model cannot be changed if the set is already attached.
Button programming	Lets you program the buttons with internal and external autodialers and/or programmed feature keys.
User speed dial	Programs user speed dialers (No defaults).
Call log options	Select whether the set will: Log all calls, No autologging, No one answered or Unanswered by me.
Dialing options	Select Standard dial, Pre-dial or Automatic dial.
Language	Choose the display language: English, French or Spanish.
Display contrast	Adjust the contrast of the display 1, 2, 3,4, 5.....9
Ring type	Select a ring type 1, 2, 3, 4

Restrictions

Restrictions prevent a user from making certain kinds of calls from a telephone or from lines that are available at the telephone. It also restricts some features.

When you are finished programming restriction settings for one telephone, you can copy those settings to other telephones.

Set restrictions

Set restrictions lets you assign a restriction filter to a telephone to prevent certain numbers from being dialed from that telephone, and prevent certain features from being used by a telephone.

Set lock

You can adjust the amount of personal programming and customizing that can be done at a telephone. Select the setting: **None**, **Partial**, or **Full**.

None allows you to access all features on your telephone.

Partial prevents:

- programming autodial buttons
- programming user speed dial numbers
- programming feature buttons
- moving line buttons
- changing the display language
- changing dialing modes (Automatic Dial, Pre-Dial, and Standard Dial)
- using Voice Call Deny
- saving a number with Saved Number Redial

Full, in addition to the restrictions outlined for Partial lock, prevents:

- changing Background Music
- changing Privacy
- changing Do Not Disturb
- using Ring Again
- using Call Forward all calls
- using Send Message
- using Trunk Answer
- activating Services

Allow last number

Click **Y** or **N** to allow a set to use the Last Number Redial feature.

Allow saved number

Click **Y** or **N** to allow a set to use the Saved Number Redial feature.

Allow link

Click **Y** or **N** to allow a set to use the Link feature, a host signaling option.

Schedules

You can assign a different restriction filter for normal service and for each of six schedules. See the section on Services for more information about the schedules. Enter the number of the restriction filter to be assigned to the set for each schedule.

Schedule	Restriction filter
Normal	02
Schedule 1 (Night)	11
Schedule 2 (Evening)	12
Schedule 3 (Lunch)	13
Schedule 4	00
Schedule 5	00
Schedule 6	00

This means, for example, that if you enter a set of restrictions for filter 11, they will be automatically applied when the Night schedule is in use.

Line / set restrictions

Line/set restrictions lets you assign a restriction filter to a specific line that can be used for outgoing calls at a specific telephone. This type of filter replaces any line or set restriction filters which might otherwise apply. It restricts the numbers you can dial on a line, but only from that telephone. The same line on another telephone can have different restrictions.

As with set restrictions, you can apply a different line restriction for normal service and for each of six schedules.

Choose **None** or **Filter:**. Enter the number to be assigned as the line/set restriction for each schedule and click **Save**. There are no default line/set restrictions.

Tips

A maximum of 255 line/set restrictions may be applied to lines at telephones.

If a line/set restriction is assigned to a line at a particular telephone, it overrides any line restrictions or set restrictions which might otherwise apply.

If no line/set restrictions have been defined, the numbers are checked against the set restrictions and the line restrictions, if either of these have been defined. The numbers may be rejected by either restriction.

Telco features

Telco features can program the way Enterprise Edge works with features and services that are based in the public network or other outside source. Enterprise Edge is designed to work with two of these kinds of services: Call Display and an external voice message service.

When you are finished programming Telco features settings for one telephone, you can copy those settings to other telephones.

Feature assignment

If you subscribe to Call Display services (often called Caller ID), external calls are identified on the display. You may also have a message indicator from an external voice mail service show on the set's display. Analog Call Display services are available with an EE-CTM. Feature assignment programming allows you to customize how this information is used.

PRI also provides the Caller ID.

Select the number of the line you want to program with Feature settings.

Call log set

Call log set allows you to specify whether the telephone automatically logs Call Display information for calls on an external line. The line must appear on that telephone, but it does not have to be a ringing line. Click **Y** or **N** to enable call logging.

Voice Message setting

If you subscribe to a voice message service, you can access that service through your Enterprise Edge system. The external voice message setting controls whether the indicator shows up when there is a voice message waiting on a particular line. The line must appear on that telephone. Click **Y** or **N** to enable voice messaging.

To find out if your voice message service will work with Enterprise Edge, or if you have any problems with your service, contact your voice message service provider.

First Display

Depending on the services you subscribe to, Call Display information may contain the number of the caller, the name of the line in your Enterprise Edge system that the call is on, or both. For each telephone, you can determine which information is displayed first. Select the setting: **Name**, **Number** or **Line**.

Tips

The Call Information feature is used to display and toggle between the name and line number used for Call Display information.

You may see **Unknown number** on the display if the information is not available from your telephone company. You may see **Private number** on the display if the caller blocks that information.

Auto called ID

Auto called ID allows you to see the extension number and name of the set being called on the display. The Auto called ID set for target lines is the same set that has appearance on that target line. Click **Y** or **N** to enable Auto called ID.

Set log space

Log space determines the number of items that can be stored in the Call log for each telephone. There is no log space assigned by default. Enter the amount for **Available log space**.

Tips

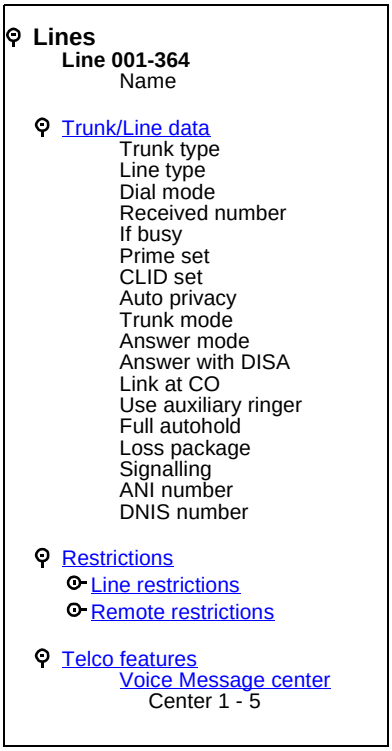
There must be space available in the log pool in order for you to add space to a Call log. The maximum number of spaces available is 600.

System-wide log space allocation is performed in Call log space under **General settings**. If you want to allocate the same log space to all telephones, use the Call log space setting instead.

Lines

The Lines heading allows you to assign settings for each line. The following illustration shows a detailed view of the Lines programming map.

Note: Lines 001 to 014 are reserved for VoIP trunks. Lines 241 to 364 are reserved for target lines.



To program settings for a line, click the line number (Line 001-364) of the line and click the key to display the programming sublevels.

Copying settings from one line to another

The Copy commands allows you to duplicate programming for a line and apply it to another line or a range of lines.

When copying data from a physical trunk to a target line (or the other way around), only the data in common is copied. For example, copying a target line to a T1 E&M trunk copies only the Line data settings because there are no Trunk data settings for a target line.

If you try to copy line programming between lines on different types of modules, the window shows an error message. You cannot copy programming between lines on different types of modules.

The Received number of a target line is a unique number and cannot be copied.

To copy settings from one line to another:

1. Choose **Resources, Telephony, Lines**.
2. Click the line (Line 001-364) from which you want to copy settings.
3. If necessary, choose a subheading to refine your selection.
4. On the **Edit** menu, click **Copy**.
5. Click **Single** from the Copy type list box.
6. Type the line number of the line to which you want to copy the settings.
7. Click the **OK** button.

To copy programming from one telephone to a range of lines:

1. Choose **Resources, Telephony, Terminals & Sets**.
2. Click the line (Line 001-364) from which you want to copy settings.
3. If necessary, choose a subheading to refine your selection.
4. On the **Edit** menu, click **Copy**.
5. Click **Range** from the Copy type list box.
6. Type the start and end line numbers of the lines to which you want to copy the settings.
7. Click the **OK** button.

Trunk/Line data

Trunk/line data lets you program settings for lines that affect how Enterprise Edge communicates with other switches, and lets you determine how lines (including target lines) will be used in the Enterprise Edge system.

To configure a trunk or line:

1. Select a trunk type: **VoIP**, **Loop**, **E&M**, **DID**, **Ground**.

   For more information about trunk types, see Trunk type on page 100.

Note: You can only change the trunk type setting for lines connected to an EE-DTM module. All other lines are automatically configured based on the type of hardware module present. VoIP is automatically assigned as the trunk type to Lines 001 to 014 and cannot be changed.

Trunk/line data settings vary depending on the type of trunk that has been programmed and the hardware to which the trunk is connected. The following table lists the options that are available for each trunk type. A checkmark indicates that the option is present.

Trunk Type	Loop start Analog	Loop start Digital	Ground start Digital	DID Digital	E&M Digital	PRI lines	Target lines	VoIP
Line type	✓	✓	✓	✓	✓	✓	✓	✓
Dial mode	✓	✓	✓	✓	✓	–	–	–
Received #	–	–	–	–	–	–	✓	–
If busy	–	–	–	–	–	–	✓	–
PrimeSet	✓	✓	✓	✓	✓	✓	✓	✓
CLID set	✓	✓	–	–	✓	–	✓	–
Auto privacy	✓	✓	✓	✓	✓	–	–	✓
Trunk mode	✓	✓	–	–	–	–	–	–
Answer mode	✓	✓	✓	–	✓	–	–	–
Answer with DISA	✓	✓	✓	–	✓	–	–	–
Link at CO	✓	–	–	–	–	–	–	–
Use auxiliary ringer	✓	✓	✓	✓	✓	–	✓	✓
Full autoHold	✓	✓	–	–	–	–	–	✓
Loss Package	✓	–	–	–	–	–	–	–
Signal	–	–	–	✓	✓	–	–	–
ANI Number	–	–	–	✓	✓	–	–	–
DNIS Number	–	–	–	✓	✓	–	–	–

2. Configure the line settings according to the table:

Attribute	Description
Line type	Specifies how the line is to be used in relation to other lines in the system. Values: Public, Private to:, Pool A to O, PRI-A to PRI-F (Default:
Dial mode [1]	Specifies whether dual tone multifrequency (DTMF) or pulse signalling is used on the trunk. Values: Pulse, Tone, (Default: Tone)
Received number	Specifies the digits to make a specific target line ring. Values: up to 24 digits (Default: blank)
If busy	Defines whether a caller gets a busy tone or the call is forwarded to the prime set when the target line is busy. Values: To Prime, Busy Tone
Prime set	Assigns a telephone to provide backup answering for calls on the line. Values: DN:, None (Default: DN 221)
CLID set	The Call Line Identifier (CLID) set prompt, specifies which sets are capable of using the feature. Values: DN:, None (Default: None)
Auto privacy	Defines whether one Enterprise Edge user can select a line in use at another telephone to join an existing call. Values: Y or N (Default: Y)
Trunk mode [2]	Defines whether or not disconnect supervision (also referred to as loop supervision) is enabled. Values: Unspr, Super (Default: Unspr)
Answer mode	Defines whether a trunk is manual or automatic answer. Values: Manual, Auto (Default: Manual)
Answer with DISA [3,4]	Defines whether a caller is prompted for a six digit class of service (COS) password. Values: Y or N (Default: Y)
Link at CO	Values: Y or N (Default: N)
Use auxiliary ringer	Allows you to turn the auxiliary ringer on or off. Values: Y or N (Default: N)
Full autohold [5]	Enables or disables full autohold. When enabled, if a caller selects an idle line but does not dial any digits, that line is automatically placed on hold if you then select another line. Values: Y or N (Default: N)
Loss package	Allows you to select the appropriate loss/gain and impedance settings for each line. Values: Short CO, Medium CO, Long CO, Short PBX, Long PBX (Default: Medium CO)

Attribute	Description
Signalling [6]	Defines the signal type for the line. Values: WinkStart, Immediate, DelayDial (Default: Winkstart)
ANI Number [7]	Defines whether the telephone number of the caller will be collected for this line. Values: Y or N (Default: N)
DNIS Numberr [8]	Defines whether the digits dialed by an external caller on this line will be collected. Values: Y or N (Default: N)

Notes:

1 Tone does not appear if Signalling is set to Immediate (T1 DID &T1 E&M trunk types only).

2 Must be set to Super if a loop trunk has its Answer mode set to Auto or Answer with DISA is enabled. Disconnect supervision is also required to conference two external callers. The line must be equipped with disconnect supervision from the central office for the Super option to work.

3 Appears for T1 loop start and T1 E&M lines that have auto-answer mode.

4 Set this option to No for T1 E&M lines on a private network that have auto-answer mode.

5 Applies to loop start and VoIP trunks. Full autohold is always in place for T1 E&M trunks; it has no meaning for incoming-only T1 DID trunks.

6 Applies to T1 E&M or T1 DID trunks. The immediate setting does not appear for T1 E&M or T1 DID trunks connected to an EE-DTM if the Dial mode is set to tone.

7 Applies to T1 E&M and T1 DID trunks. For T1 E&M and T1 DID trunks connected to an EE-DTM, this setting only appears if Signalling is set to WinkStart.

8 Applies to T1 E&M trunks. For T1 E&M trunks connected to an EE-DTM, this setting only appears if Signalling is set to WinkStart and Answer mode is set to Manual.

Trunk type

The Trunk/line data displayed in the Unified Manager will vary with the type of trunk module, how it is configured, and which line is selected. For example, the EE-DTM can be configured as PRI or T1. For more information, see Hardware on page 175. To enable or disable a module, consult the Maintenance chapter.

The following trunk types can be programmed:

Hardware Unit	Trunk Types
EE-DTM	PRI T1 Loop, T1 E&M, T1 Ground
EE-CTM	Loop

Enable modules

If you disabled any Trunk Modules to perform programming, enable them now using **Module/ port status** in **Maintenance**, or your system will not function properly. See Module/port status on page 254.

Voice over IP trunk considerations

For IP functionality with Enterprise Edge VoIP Gateway, the trunk type is **VoIP.** Enterprise Edge VoIP Gateway routes voice traffic over private Internet Protocol (IP) networks to link multiple sites together using an existing corporate data network. Lines 001 to 014 are reserved for IP functionality. The number of lines available for use is a function of software key codes and currently eight of the fourteen lines are available for IP functionality.

Note: VoIP trunks should not be accessed through Line appearances as the user will not receive dial tone.

VoIP trunks should be configured to use PRI pool A. This way, you can configure your IP trunks to use the fallback feature.The use of Line pool codes is not recommended as you will not be able to configure for fallback. The quality of the IP trunk connection is assessed during initial call setup, and if the quality is above the configured threshold, Enterprise Edge will try to find an alternate route to complete the call (fallback) based on the programming definitions in the routing table. If you do not configure your network for fallback and the call quality is below threshold, the IP call will fail. For an example of a network configuration that supports fallback, see Toll bypass with Enterprise Edge VoIP Gateway on page 325.

When fallback is configured, the IP call will be rerouted to a circuit-switched connection. This could be either a private network trunk or it could be a public network trunk. Ideally you would want to configure fallback to use the least cost route if possible. For more information about configuring VoIP trunks, see the *Enterprise Edge IP Telephony Configuration Guide*.

Tips

VoIP requires 7 digit dialing. If you use less than 7 digits, users must enter a # sign to indicate that they have completed their dialing. For more information, see Dialing timeout on page 125.

Line type

This setting specifies how the line is to be used in relation to other lines in the system. Select the setting: **Public**, **Private to:**, or **Pool** (A to O, representing 15 line pools) or **PRI-A** to **PRI-F**.

- A Public line can be accessed by more than one telephone.
- A Private line can be assigned only to one telephone and the prime telephone for that line. Enter the internal number of the telephone.
- Pool assigns the line to one of the fifteen line pools. If a line is assigned to a line pool, but is not assigned to any telephone, that line is available only for outgoing calls.

Tips

Line pools must never contain a mixture of lines. All lines in a given line pool should go to the same location.

Try to avoid putting unsupervised loopstart lines in a line pool. These lines can become hung, especially when a remote user uses the line pool to make an external call.

There are two more programming settings that must be assigned before a line pool can be used:

- You must assign line pool access to telephones in **Line access** programming.
- You must assign system-wide line pool access codes in **General settings** (not applicable to PRI pools).

Tips

A telephone can be administered to search automatically for an idle line from several lines appearing on the telephone. Assign a line pool as the prime line (in **Line access**) and all the lines in the line pool must appear on that telephone. When the user lifts the receiver or presses Handsfree/Mute, any one of the lines, if idle, can be selected by Automatic Outgoing Line selection.

Changing the settings for trunk type on a system that is in use, may cause calls to be dropped.

When assigning lines to line pools, consider your network configuration. You may be able to create a unified dialing plan by assigning lines to the same location to the same line pool on each of your systems. For example, if system A and system B each have tie lines to system C, assign the tie lines to pool D on each of the systems.

You cannot assign target lines to a line pool.

Dial mode

Dial mode lets you specify whether dual tone multifrequency (DTMF) or pulse signalling is used on the trunk.

Received number

The Received number setting applies only to target lines. It allows you to specify the digits to make a specific target line ring. The default value is blank.

A received number cannot be the same as, or be the start digits of a line pool access code, a destination code, the DISA DN or the Auto DN.

If busy

When a call is received on a target line that is already busy, you can choose if the caller get a busy tone or if the call is forwarded to the prime set. Busy tone only works for PRI trunks.

Prime set

This feature allows you to assign a telephone to provide backup answering for calls on the line. Unanswered calls are redirected to the prime set. For an Auto Answer line, calls will be redirected if the received number is invalid or the target line is busy, and if the 'If busy' parameter is set '**To prime**'.

Enter the DN number of the prime set or select **None**. The default prime set for each line is **221**.

Note: Each line can be assigned only one prime set.

CLID set

An Enterprise Edge set displays the telephone number of the calling party. The Call Line Identifier (CLID) set prompt, lets you specify which sets are capable of using the feature.

Auto privacy

This feature controls whether one Enterprise Edge user can select a line in use at another telephone to join an existing call. The default setting is Privacy on, so that nobody with an Enterprise Edge telephone can press a line appearance on their telephone to join a call in progress at another telephone.

Tips

Users can change a line's privacy setting for an individual call using the Privacy feature (Feature 8 3).

Trunk mode

Trunk mode lets you specify one of two modes of operation for each line: disconnect supervision or unsupervised. Disconnect supervision, also referred to as loop supervision, releases an external line when an open switch interval (OSI) is detected during a call on that line. This prevents the line from remaining unavailable for other Enterprise Edge users.

- **Unspr** (the default) turns disconnect supervision off for the line.
- **Super** assigns supervised mode, if supported by the line; otherwise, the line functions as unsupervised.

Tips

The duration of an open switch interval (OSI) before Enterprise Edge disconnects a call is programmed by the **Disconnect timer** setting. See Hardware on page 175 for more information.

Answer mode

The Answer mode setting appears for T1 ground start lines, T1 E&M lines, and T1 loop start lines whose Trunk mode setting is set to Super. Select the setting: **Manual** or **Auto**.

Note: Disconnect supervision is required if loop start trunks are to operate in auto-answer mode.

Answer with DISA

The Answer with DISA setting is used to prompt a caller for a six digit class of service (COS) password. The caller will hear a stuttered dial tone when the phone is answered, and must then enter the password digits.

To program DISA on a PRI trunk, see Direct inward system access (DISA) on page 310.

Link at CO

Some exchanges respond to a Link signal (Feature 7 1) by providing an alternative line for making outgoing calls. When Link at CO is enabled, the system applies the restrictions on outgoing calls to the digits dialed after the Link signal, and the call on the alternative line will be subject to all restrictions. Disabling Link at CO prevents a Link signal from resetting the Enterprise Edge restrictions in cases where the host exchange does not provide an alternative line.

Use auxiliary ringer

This setting allows you to turn the auxiliary ringer on or off. An auxiliary ringer can be programmed on a line or a set. When programmed on a line, the auxiliary ringer will ring every time a call is received. When programmed only on a set, the auxiliary ringer will not ring when a transferred call is received.

Tips

The auxiliary ringer is an optional device that should be connected by the installer.

If you have an auxiliary ringer programmed to ring for calls on an external line, and you transfer a call on that line without announcing the transfer, the auxiliary ringer will ring for the call transfer.

An auxiliary ringer can also be programmed in Services to ring for a line placed into a scheduled Ringing service.

Full autohold

Full autohold on idle line is a variation of the Automatic Hold feature. If you select an idle line, but do not dial any digits, that line is automatically placed on hold if you then select another line.

The line you first selected is held until you press its button. The line is not available for use by anyone else.

Note: The default setting should be changed only if Full autohold is required for a specific application.

Loss package

Loss package lets you select the appropriate loss/gain and impedance settings for each line. The setting is based on the distance between Enterprise Edge and the terminating switch, and the terminating switch type. When measuring the distance from Enterprise Edge to CO and from Enterprise Edge to PBX, use 600 ohms as the termination resistance setting.

Loss Package	Receive Loss	Transmit Loss	Impedance	Distance to switch / cable loss / terminating switch
Short CO	0 dB	3 dB	Short	Short/<2 dB/Enterprise Edge to CO
Medium CO	0 dB	0 dB	TIA/EIA 464	Medium/>2 dB and <6 dB/ Enterprise Edge to CO
Long CO	-3 dB	0 dB	TIA/EIA 464	Long/>6 dB/Enterprise Edge to CO
Short PBX	0 dB	0 dB	Short	Short/<2 dB/Enterprise Edge to PBX
Long PBX	-3 dB	0 dB	TIA/EIA 464	Long/>2 dB/Enterprise Edge to PBX

A loss of 4 dB corresponds to a cable length of approximately2700 m (9000 ft.)

Signalling

Select the signal type for the line: **WinkStart**, **Immediate** and **DelayDial**.

The Signal setting appears on the window only for T1 E&M or T1 DID lines.

Make sure that this matches the signal type programmed for the trunk at the other switch.

For T1 E&M and T1 DID lines on an EE-DTM (DTI), the Immediate setting does not appear if dial mode for the line is tone.

ANI Number

Select whether the telephone number of the caller will be collected for this line. The digits can then be displayed on Enterprise Edge telephones as part of Call Display services.

The central office must deliver ANI/DNIS in DTMF mode.The delivery of ANI/ DNIS depends on the network provider and the services they offer.

If the conditions for signalling mode and start arrangement are not met, prompts are not presented to the user. No additional equipment is required.

DNIS Number

Select whether the digits dialed by an external caller on this line will be collected.

This setting applies to T1 E&M lines only.

For T1 E&M lines on an EE-DTM, this setting only appears if Signal is **WinkStart** and Answer mode is **Manual**. These digits are required for some third party software applications.

Name

The default name for a line is “Line” and its three-digit number (for example, Line 001), but it can be changed to any combination of letters and numbers to a maximum length of 7 characters. Click on a line number in the Unified Manager and enter the name in the **Name** field.

Restrictions

Restrictions prevent a user from making certain kinds of calls from lines that are available at the telephone. It also restricts some features.

Line restrictions

Specify the filter to be applied to this line to restrict the numbers that can be dialed on it. You can assign a different restriction filter for normal service and for each of six schedules. See the section on Services for more information about the schedules. For PRI, all line restriction changes are applicable to all 23 lines.

Enter the number of the restriction filter to be assigned as the line restriction for each schedule. The default restrictions are as follows:

Schedule	Restriction filter
Normal	03
Schedule 1 (Night)	21
Schedule 2 (Evening)	22
Schedule 3 (Lunch)	23
Schedule 4	00
Schedule 5	00
Schedule 6	00

Tips

When a remote user places an external call on a line, any filters used with the line still apply.

Remote restrictions

Specify the restriction filter to be applied to remote callers calling in to the Enterprise Edge system on this line. A restriction filter is a set or group of restrictions and overrides.

As with line restrictions, you can apply a different remote restriction for normal service and for each of six schedules. Select the remote restrictions for each schedule. The default restrictions are as follows:

Schedule	Restriction filter
Normal	04
Schedule 1 (Night)	31
Schedule 2 (Evening)	32
Schedule 3 (Lunch)	33
Schedule 4	00
Schedule 5	00
Schedule 6	00

Tip
The remote restriction restricts the numbers that can be dialed on an incoming auto-answer line. If a remote user then selects a line to place an external call, any filter used with the line still applies.

Telco features

Voice Message center

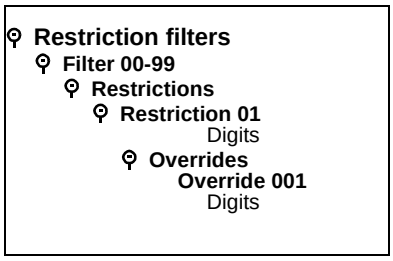
If you subscribe to a voice message service, you can specify which voice message center is used for each external line that can receive message waiting indication. For each line, select the setting:
Center1 through **Center 5**, or **None**.

Enter the telephone numbers for each of the five voice message centers (if required).

Restriction filters

Restriction filters prevent a user from making certain kinds of calls from a telephone or from lines that are available at the telephone. They also restrict some features.

The following illustration shows detailed view of the Restriction filters programming map.



Filters

A restriction filter is a set or group of restrictions and overrides that specify the external numbers or feature codes that cannot be dialed from a telephone or on a line. Rather than define individual restrictions and apply them repeatedly to telephones and to lines, restriction filters let you assign them in one step as a single package of dialing sequences that are not permitted.

In addition to restricting telephone numbers, you can prevent people from entering dialing sequences used by the central office (the public network) to deliver special services and features. Because some of these features provide the caller with dial tone after they have entered the special code (which often uses # or *), users may have an opportunity to bypass restrictions. To prevent this from happening, you should create filters that block these special codes.

You create a filter by defining the dialing sequences that are denied. There will also be variations of each sequence that you will want users to be able to dial. Sequences that can be dialed are called overrides.

Once you create the filters, you can assign the restrictions to a telephone (under **Terminals & Sets**), to a line (under **Lines**), to a particular line on a telephone (under **Terminals & Sets**), and to remote callers (under **Lines, Remote access**).

1. Select the number of the restriction filter you want to program.
2. The restrictions are displayed in the right window.
3. Enter a restriction for each filter.
4. View any overrides to the restriction.
5. Enter overrides for each restriction filter.

6. Enter the letter '**A**' as a wild card character that represents any digit in a sequence of numbers when denying numbers or creating overrides.

7. You can delete a restriction.The overrides will be deleted as well and the restrictions will renumber to fill the gap.

Default filters

Filter 00 permits unrestricted dialing and cannot be changed.

Filter 01 is pre-programmed with five restrictions and some associated overrides. In Filter 01, restriction 02 and override 005 allow long distance directory assistance calls. Filter 01 reflects the fact that area codes can now have any digit as a second digit. This is designed to be used with the North American dialing plan.

The dialing string 911 (the number for emergency assistance in North America) is included as both a restriction and an override in filter 01. This arrangement prevents anyone from blocking calls for emergency assistance on lines or sets using the default filter.

Filter	Restrictions (denied)	Overrides
00	Unrestricted dialing	
01	01: 0	
	02: 1	001: 1800 002: 1877 003: 1888
	03: 911	001: 911
	04: 411	
	05: 976	
	06: 1976	
	07: 1AAA976	
	08: 1900	
	09: 1AAA900	
	10: 5551212	
02 - 99	No restrictions or exceptions programmed	

Note: Default filters are only loaded at a cold start.

Filters 02, 03, and 04, although not preset with restrictions and overrides, are used as default filters in these programming headings:

Filter	Heading	Sub-heading
02	Terminals & Sets	Set restrictions
03	Lines	Line restriction
04	Lines	Remote restriction

Tips

Filter 00 cannot be changed. Enterprise EdgeE. can have up to 100 restriction filters (00 to 99).

Each programmable filter can have up to 48 restrictions. There is no limit on the number of overrides that can be allocated to a restriction. There is a maximum of 400 restrictions and overrides allocated to the 100 programmable filters.

The maximum length of a restriction is 15 digits. The maximum length of an override is 16 digits.

A single letter (A) in a dialing sequence is a wild card (stands for any digit). You can use * and # in a sequence of numbers in either a restriction or an override. These characters are often used as part of feature codes for other systems or for features provided by the central office (the public network).

When restricting the dialing of a central office feature code, don't forget to create separate restrictions for the codes used for DTMF and pulse lines. Examples of dialing strings that may be restricted for this reason are *67 and 1167. Do not string together a central office feature code and a dialing sequence that you want to restrict. Create a separate restriction for each.

You can copy restrictions and overrides from one filter to another. Any restriction or override can be used in any number of filters. Each time it is used, it counts as one entry. For example, if restriction 411 exists in filters 01, 02 and 03, it uses up three entries of the 400 entries available.

Removing a restriction from a filter has no effect on the contents of other filters even if the restriction was copied to them. You cannot delete a filter. Removing the restrictions programmed on a filter makes it an unrestricted filter but the filter itself is not removed.

Exercise caution when removing overrides

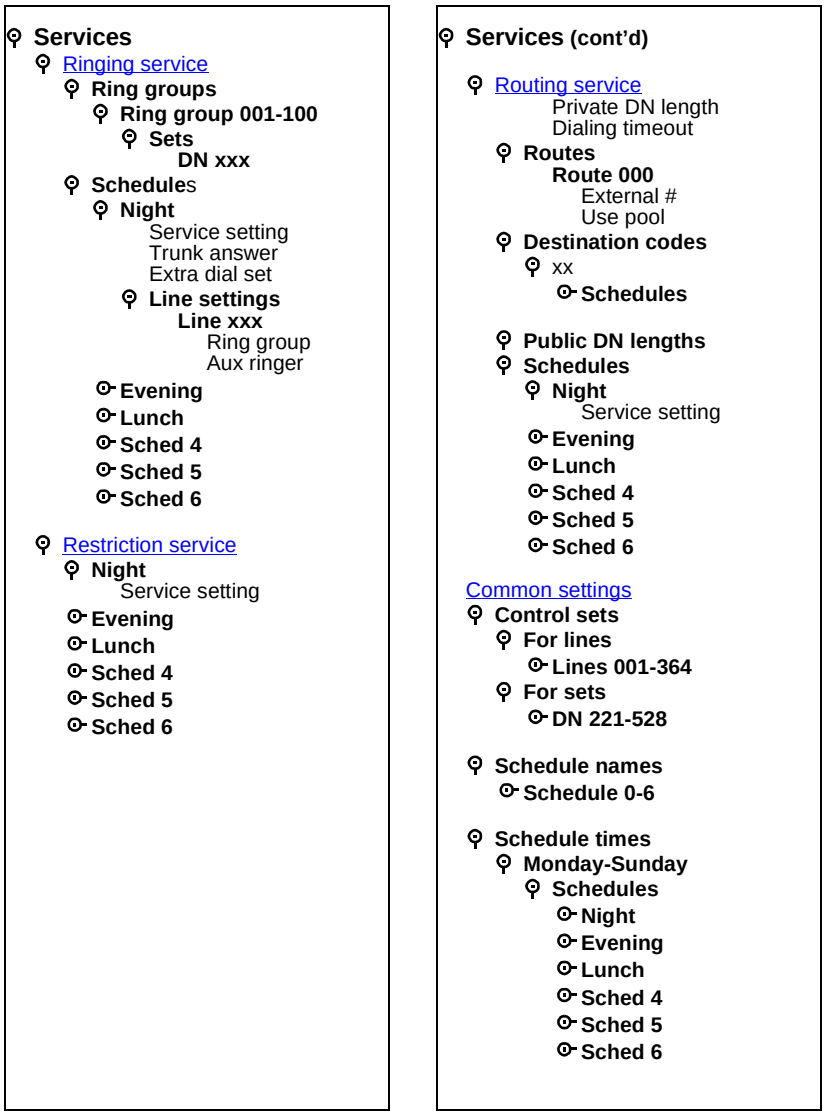
Removing a restriction removes the overrides associated with it. It also changes the identifying numbers of the subsequent restrictions that you may have defined. For example, if you remove restriction 01, restrictions 02 to 08 are renumbered as 01 to 07.

Services

The Services heading allows you to control three types of service by the time of day and day of week:

- alternate call ringing for certain times and days
- alternate dialing restrictions for certain times and days
- alternate call routing for certain times and days.

The following illustration shows a detailed view of the Services programming map.



Each of the three services has six schedules that you can customize. For example, you may want to combine alternate call ringing with alternate dialing restrictions for lunchtime, evenings, and weekends (Schedules 1, 2, and 3). Then you may want to run alternate call routing using three separate schedules.

Tips

Once you have programmed the different services and schedules, you can turn each of the services on separately. For example, the Night schedule might control both Ringing service and Restriction service. But you can turn on just the Ringing service part of the Night schedule if you wish.

You can activate the services from the designated control telephone for each Enterprise Edge telephone and line in your system. You can have one control telephone for the whole system, or different control telephones for different Enterprise Edge telephones and lines.

If you want to have several services active at the same time, simply program them on for the same schedule.

Ringing service

At certain times or in certain situations, you may want additional telephones to begin ringing for incoming lines. The most common use of this feature is when a security desk telephone begins to ring for incoming lines after 5:00 p.m., a practice often called “night service”.

Ring groups

Ring groups allows you to define groups of extended ringing sets. A group can be assigned to any line for any of the schedules. You can create up to 100 ring groups composed of up to 30 sets for each ring group.

To define a ring group enter the number of the group you want to program (001-100). Once you define a ring group, enter the number of the set you want to assign to this ring group.

Tips

You can assign any set on the Enterprise Edge system to a ring group. The assigned control set for each schedule is added to each ring group.

A set can belong to more than one ring group.

Schedules

Indicate how Ringing service should be activated for each of the schedules.

Service setting

Click on a schedule such as Night and select the setting for that schedule: **Off**, **Auto**, or **Manual**.

Manual allows you to turn the service on and off at any time from a control set using the Ringing service feature code.

Automatic allows you to program a stop and start time for a service. You are still able to start and stop the service by entering the appropriate Services feature code at a control set. If you select this setting, you will have to set start and stop times. See the section on schedule times for information on programming times.

Off prevents the service from being activated.

Trunk answer

Trunk answer allows you to answer, from any telephone, an external call that is ringing at another telephone in your office. This is useful if the other telephones have not been assigned the same lines as the telephone you are using to answer the call.

Click **Y** or **N** to enable Trunk answer.

Tip
You can change the Trunk Answer setting only if Ringing service is set to Manual or Automatic.

Extra dial set

Extra dial set allows you to assign an additional direct-dial set in the Enterprise Edge system for each schedule you use.

Enter the internal number of the extra-dial set or choose **None**.

Tip
The extra dial set is activated during a schedule by entering the Ringing service feature code from a direct-dial set. This does not activate the Ringing service unless the direct-dial set is also a control set.

Line settings

For Ringing service, **Ring group** and **Auxiliary ringer use,** are programmed for each line individually.

Ring group - You can assign a predefined ring group to a line for each schedule. See Ring groups on page 112 to create groups of extra ringing telephones.

Select the line number to see which ring group is assigned to the line. Select the ring group number (001-100) to choose a different ring group assignment.

Tip
Only one ring group can be assigned to a line for each schedule. To combine groups of ringing sets, you must create a new ring group which contains all the sets you want to ring and assign it to the line.

Auxiliary ringer - Indicate whether the auxiliary ringer (if installed) also rings when Ringing service is on. Click **Y** or **N** to enable Auxiliary ringer.

Tips

The default ringing telephone is 221. This means that all lines ring at telephone 221 when Ringing service is on.

You can copy Ringing set and Auxiliary ringer programming from one line to another.

If you have an auxiliary ringer programmed to ring for calls on an external line, and you transfer a call on that line without announcing the transfer, the auxiliary ringer will ring for the call transfer.

Restriction service

Indicate how the alternate dialing restrictions should be activated for each of the schedules. Select the schedule e.g. **Night**, and the **Service setting**.

Select the service setting for each schedule: **Off**, **Automatic**, or **Manual**.

See Ringing service in this section for descriptions of the three settings.

Routing service

The programming for routing decides what path an outgoing call takes using the digits that are dialed. It is sometimes called Automatic Route Selection (ARS).

When you select an internal line and dial, the numbers you enter are checked against the routing tables. If the number you dialed starts with a destination code, the system uses the line pool and dials out digits specified by the route assigned to that destination code, and then dials the rest of the number that you dialed.

Routing service replaces a number of tasks that otherwise have to be done manually, including:

- entering a line pool code
- dialing an access code for a long distance carrier
- deciding which line pool to use according to the time and day

You can set up routing to take advantage of any leased or discounted routes using information supplied by the customer. The system itself cannot tell which lines are cheaper to use.

For Call by Call service selection (PRI only), the installer defines destination codes for various call types over PRI lines (e.g. Foreign Exchange, Tie Trunk, and OUTWATS). The user simply dials a number via the intercom button without having to enter any special information. For more information see, Call by Call service selection for PRI on page 151.

Using routing to create a coordinated dialing plan is explained in Coordinated dialing plan on page 310.

Plan your routing service before doing any programming.
Routing affects every call placed in the system and must be carefully planned to avoid conflicts and gaps in the programming. Use tables to design routes and destination codes, then check for potential problems before you start programming. It will also save you time to have all the settings written out in front of you.

Routes and destination codes

Programming for a route makes use of:

- a 3-digit route number (000-999)
- External # digits (up to 24)
- a line pool
- destination codes (max. of 500 available, up to 7 digits)
- Public DN lengths
- a schedule (programmed in Services)

Tips
To dial a telephone number which does not match any of the programmed destination codes, the user will have to choose a line and dial the number. For long distance dialing, area codes in the North American numbering plan can be programmed as destination codes.

Route

Select **Routing Service, Routes**. Click **Add**. Enter a 3 digit route number (000-999) and click **Save**.

External

External number or dial out number is the number you want the route to use. Enter the digits (up to 24). You can press F78 to insert a 1.5 second pause in the dialing string, or F804 to wait for dial tone, if necessary. Route 000 has no External # by default and cannot be changed.

Use Pool

Select a line pool to be used with the route: **Pool A**, **Pool B...Pool O** or **PRI-A to PRI-F**. The PRI pools will only be displayed if an EE-DTM has been configured for PRI.

Route 000 uses Pool A by default and cannot be changed.

Call by Call Service routing

The following is an example of a Routing Table containing Call by Call programming.

Route # (000-999)	Dial Out (24 digits)	Use Pool	Service Type	Service Identifier
003		PRI-A	Public	
004		PRI-A	FX	xxxxx
005		PRI-A	Tie	xxxxx
006		PRI-B	OUTWATS	xxx
007		PRI-B	Private	
008		PRI-B	Switched Digital	
Note: The public DN lengths are used for all PRI calls except those whose routes use service type Private or service type Tie with DN Type specified as Private.				

The service identifier (SID) depends on the selected service type.
(For example with NI-2 protocol)

Service Type	Service Identifier description
Public	None
FX	Facility Number 1-5 digits
Tie	Facility Number 1-5 digits
OUTWATS [a]	Optional Band Number 1-3 digits
Private	None
Switched Digital	None
a. For NI-2, do not program the Carrier Access Code for banded OUTWAT calls. This call may be rejected.	

When a PRI protocol is selected or changed, the Service Type and Service ID fields are automatically cleared for each entry in the routing table for that PRI.

Programming the PRI routing table

The dialing plan must be thoroughly planned out in advance before programming the information into the Enterprise Edge system.

Programming the routing table takes place in **Services** under **Routing Service: Routes**

1. Under **Route001, External #: No number**, enter a number (up to 24 digits).

2. Under **Use pool:** select a line pool.
   The PRI pool(s) displayed depend on how the PRI lines are put into pools in the Trunk/Line data section of programming. It is possible to have only pool PRI-A or only pool PRI-B or only PRI-C etc. up to PRI-F, even if there are three EE-DTMs configured as PRI in the system.

3. Under **ServiceType:Public**. Select a different Service Type if required.

4. Under **Service ID:None**. Enter the Service ID number. This is shown only if the service requires an ID.

5. Under **DN type:Public**. Enter **Public** or **Private**. This is shown only for service type Tie.

Destination codes

The numbers used for destination codes must not conflict with:

- Call Park Prefix
- External Access Code
- Direct Dial Numbers
- Line Pool Code
- Internal set numbers (intercom)
- DISA set numbers
- Auto DNs

For example, the system will confuse an internal number of 221 and a destination code of 22 because even if the caller dialed the complete internal number, the call would be routed using the first two digits. But an internal number of 221 and a destination code of 23 would work.

In order to make digits available for use with destination codes, you must change the DN length of B1 and B2 DNs depending on your system size. This can be done either at system startup or in **General settings**.

Wild card character

When programming destination codes, you can use wild cards in the destination code string. As a result of wild card characters, the number of destination codes programmed in the system is reduced thus maximizing the use of destination codes in the system.

1. At **Destination codes**, enter the destination code you want to modify or enter a new destination code.

2. When you enter a destination code, enter the letter 'A' as a wild card character in the destination code.

The wild card character can be used only for the last digit of a destination code and represents any digit from 0 to 9 except for digits already programmed or used by other numbering plans. Should there be a conflict with other digits already programmed or used by other destination codes, the digit will not be displayed.

The wild card character can only be used to group destination codes that use the same Route and Digit Absorbed Length.

Route	External #	Line Pool
555	763-4018	Line Pool C
565	763-3492	Line Pool A

Destination codes	Route	Digit Absorb	Dial Out
9201	555	3	763-4018 *-1*
9202	565	3	763-3492 *-2*
9203	555	3	763-4018 *-3*
9204	555	All	763-4018
9205	565	2	763-3492 *-05*
9206	555	3	763-4018 *-6*
9207	555	3	763-4018 *-7*
9208	555	3	763-4018 *-8*
9209	555	3	763-4018 *-9*

Note: The numbers in italics in the Dial Out sequence are not visible to the user.

Destination codes	Route	Digit Absorb	Dial Out
920A	555	3	763-4018 - A
9204	555	All	763-4018
9205	565	2	763-3492 - *05*

Note: The numbers in italics in the Dial Out sequence are not visible to the user.

Normal route

Select which route a call using the destination code takes during normal service and for each of the schedules. The automatic schedule times are programmed under **Services**. The default Normal route is 000, which has no External # digits and uses Pool A.

Digit Absorption
Select the portion of the destination code that is always absorbed by the system and not used in the dialing sequence. Select the number of digits to be deleted: **0, 1, 2, 3, 4, 5, 6,** or **All**.

Tips
The digit absorption setting (**Digit absorb**) only applies to a maximum of two schedules. Setting digit absorption to 0 minimizes the effort involved in preparing destination codes. With a 0 setting, the actual digits dialed by a caller are preserved in the dial out sequence. Programming a dial out sequence as part of the route may or may not be necessary depending on the required dialout.

Setting up a route for local calling

An office may have different suppliers for local and long distance telephone service. By programming a destination code, any call that begins with 9 (the most common dial out digit) will automatically use lines dedicated to local service.

The first step is to build a route (under **Routing Service** in **Services**).

- enter 001 (or any other available route number)

You can view defined routes or erase a defined route.

- assuming that the lines for local calling have been placed in Line pool A, choose it as the line pool
- enter the dial out digits (if any) which are needed to direct the call once it is connected to an external line

The second step of programming is setting up how the route will work with a destination code. Because users will dial 9 to make an external call, 9 should be the destination code.

For local calls only, there are no dial out numbers (compare with Setting up a route for long distance calling on page 120).

- Enter 9 at **Destination Code:**

If entering a code other than 9, a valid destination code must be used. See Destination codes on page 117.

View existing destination codes before entering a new code.

The destination code can use a different route depending on a Schedule (see Services). In the current example, Route 001 is used when someone dials 9 during normal mode (the mode used when the other Schedules are turned off).

- The route for the first schedule appears after **Normal:**. Enter the defined route number 001.

The following illustrations show sample tables used for planning and recording routing service. They are filled out to match the examples of routes for local and long distance calling.

Routing Service (Services: Routing Service)

Route # (000-999)	**Dial out** (if required) (max. 24 digits or characters)	**Use Pool**
001	*none*	(A) B C D E F G H I J K L M N O
002	*none*	A (B) C D E F G H I J K L M N O
		A B C D E F G H I J K L M N O
		A B C D E F G H I J K L M N O
		A B C D E F G H I J K L M N O

Destination codes (Services; Routing service; Destination codes)

Service Schedule name (max. 7 char)	**Normal Rte**		**Night Rte**		**Evening Rte**		**Lunch Rte**	
DestCode (max. 7 digits)	**Use route** (000-999)	**Absorb Length**	**Use route** (000-999)	**Absorb Length**	**Use route** (000-999)	**Absorb Length**	**Use route** (000-999)	**Absorb Length**
9	~~000~~ *001*	All		All		All		All
1	~~000~~*002*	~~All~~ *0*		All		All		All
	000	All		All		All		All
	000	All		All		All		All

Setting up a route for long distance calling

An office may have leased lines or T1 E&M trunks which make it cheaper to call long distance. The routing should take place automatically when the number of the outgoing call begins with 1.

Again, the first step is to define a route (under **Services** in **Routing service**).

- enter 002 (or any other available route number) at **Route:**
- assuming that the discounted lines for calling long distance have been placed in Line pool B, choose it as the line pool
- enter 1 at **Destination Code:**

A valid destination code must be used. See Destination codes on page 117. View existing destination codes before entering a new code.

The destination code can use a different route depending on the Schedule. In this example, the system uses Route 002 (which uses Line pool B) to take advantage of the lower cost when the system is in normal mode.

- The route for the first schedule appears: **Normal:**. Enter the defined route number 002.

Tips

The digit absorption setting (**Absorbed Length**) only applies to a maximum of two schedules.

Setting **Absorbed Length** to 0 minimizes the effort involved in preparing destination codes. With a 0 setting, the actual digits dialed by a caller are preserved in the dialout sequence. Programming a dial out sequence as part of the route is not necessary.

If rates change depending on the time of the day or week, a different route can be used for the same destination code 1 when a particular schedule is in use. See Programming for least cost routing on page 122.

Adding a long distance carrier access code

In many cases, long distance service uses the same lines as local service but is switched to a specific carrier using an access number (sometimes called an equal access code). Programming for routing can include the access number so users don't have to dial it every time they make a long distance call.

1. Create a route that uses a line pool containing local lines only.

2. Program the route to use a line pool containing the lines used to access the long distance carriers.

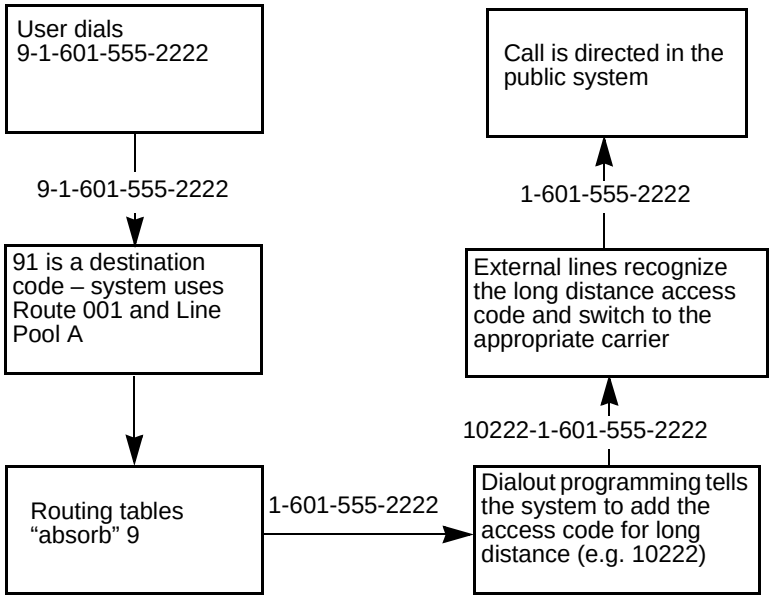
3. Enter the dial out digits, which are the same as the access digits. For example, if the access code was 10222, the dial out digits would be10222.

4. Create a destination code 91: 9 (for outside access) and 1 (for long distance). A valid destination code must be used. See Destination codes on page 117.

5. Set **Absorbed Length** to 1. The 9 is only used internally and should be dropped; the 1 is needed to direct the call to the public carrier network.

Tips

The destination codes 9 and 91 used in the examples cannot be used together. If the destination code 91 is needed to direct long distance calls, you must create a separate set of codes that use local calling routes. These codes would be, for example, 90, 92, 93, 94, 95, 96, 97, 98 and 99. See Wild card character on page 118 for information on programming destination codes.


User dials
9-1-601-555-2222
9-1-601-555-2222
91 is a destination code – system uses Route 001 and Line Pool A
Routing tables "absorb" 9
1-601-555-2222
Dialout programming tells the system to add the access code for long distance (e.g. 10222)
10222-1-601-555-2222
External lines recognize the long distance access code and switch to the appropriate carrier
1-601-555-2222
Call is directed in the public system

Programming for least cost routing

It may be cheaper to use another long distance carrier at another time of day. Continuing with the example used in the previous flowchart, the lines that supply local service in normal mode will also be used for long distance service after 6 p.m. because that is when rates become competitive. For the system to do this automatically, another route has to be built.

1. Choose Route 007 (or any other available route) at **Route:**.

2. Choose **No number** for the dial out.

3. Choose **Line pool A** (local service carrier lines).

In this case, the change in route uses the start and stop times for Night Schedule (the schedule for different modes are set up under **Services**).

1. Enter 91 at **Destination Code:**

2. Make sure **AbsorbLength** is set at 1.

3. The route programmed with the access code as its dial out (Route 001) remains as the route used by **Normal:**

4. Under **Night route:** select **Route 007**.

Calls that begin with the digits 91 will now travel out without using the access code when the Night schedule comes into use automatically or when it is turned on at a control telephone.

Service setting

Change the service setting for each schedule: **Off**, **Automatic**, or **Manual**.

See Ringing service on page 112 for descriptions of the three settings.

Overflow routing

If all the lines used by a route are busy when a call is made, the mode may be programmed to overflow to the route used for normal mode. If this happens, the set will sound a warning tone and display the message **Expensive route**. The caller can then release the call to avoid using the normal route, or continue with the call.

Overflow routing is turned on or off for each Schedule in Schedule programming. Click the checkbox to enable Overflow routing.

Tips

A schedule must be active for overflow routing to be in effect. Overflow routing is not available in normal mode.

You must create an overflow route to be used with each destination code. In this way, every route used with a scheduled mode that has overflow service must have an alternate route in normal service.

Using dialing restrictions with routing

Routing service can be further customized by adding dialing filters to lines in line pools. Filters restrict the use of the line to specific area codes.

Tips

Host system signaling codes can be part of the dial out.

You can also use routing as an alternate method for a direct-dial number. For example, create a destination code 0 and program the number of the internal or external destination as the dial out. Digit absorption should be set to 1.

Because overflow routing directs calls using alternate line pools, a call may be affected by different line filters when it is handled by overflow routing.

Using a dialing plan to route outgoing PRI calls

The Dialing Plan supports PRI connectivity to public and private networks. The dialing plan is a collection of features responsible for processing and routing outgoing calls. All PRI calls must go through a dialing plan.

The Dialing Plan

- allows Enbloc dialing by buffering user-dialed digits until a complete DN has been dialed (Enbloc dialing is a requirement for PRI)

- provides the ability to map user-dialed digits to a service type on a Call by Call basis
- allows long distance carrier selection via user-dialed Carrier Access Codes
- allows incoming calls to be routed according to the service type and the digits received

Enbloc dialing

The Private DN Length must be set to the number of digits users dial to reach other nodes in the private network. The Private DN Length parameter is used by the PRI trunk to determine when a complete number has been dialed. The PSTN DN Length Table is used by the PRI trunk to determine when a complete PSTN DN has been dialed. Entries in the table consist of two fields, Prefix and DN Length.

Carrier codes

A multi-digit Carrier access code contains an Equal Access Identifier Code followed by a Carrier Identification Code. The CIC identifies the carrier to be used to handle the call. The Carrier Access Code table stores the CAC digit pattern that you define for your region. In most cases it is not necessary to change the default values. The capability is there to modify overall patterns if required.

- you can define at most five entries
- two entries will be pre-defined in North America, but you are free to remove these defaults
- each entry consists of an equal access identifier code prefix (one to six digits) and a carrier identification code length (one digit, 1 - 9)
- each entry is identified by the prefix digits themselves

1. Select **General settings, Access codes, Carrier codes, Prefix:10**.
2. Enter a **Code prefix** (1 - 6 digits).
3. Under **ID length:**, enter a carrier ID length value (one digit, 1 - 9).

Public DN lengths

- In most cases it is not necessary to change the default values. The public DN lengths table is used for all PRI calls except those whose routes use service type Private or service type Tie with DN Type specified as Private. The public DN lengths table allows Enterprise Edge to determine the length of a DN based on the initial digits dialed by the user. In the public DN lengths table
- you can define at most 30 entries
- each entry consists of a DN prefix string (1 to 10 digits) and a length value (two digits, 1 - 25)
- several entries will be pre-defined in North America (can be removed or

modified). These defaults will handle most regions in North America without the need for additional programming.

- the table always contains one ‘default’ entry; this cannot be removed. You can only modify the length parameter associated with this entry. The default entry specifies the length of any dialing string that does not match one of the other table entries.

1. Under **Routing service, Public DN lengths, Prefix default:** Select a prefix (0, 00, 01, 011, 1, 411, 911).

2. Under **DN prefix:** enter the DN prefix number (2 digits, 1 - 25).

3. Under **DN length:** enter a DN length number (2 digits, 1 - 25).

Private DN lengths

The Private DN lengths parameter specifies the length of DNs in the private dialing plan. This is used by all PRI calls where the route uses DN Type: Private.

1. Under **Routing service, Private DN lengths:x**.

2. Select a different DN length (3..10).

Schedules

Indicate how the alternate routing should be activated for each of the schedules.

Dialing timeout

Dialing timeout specifies how long Enterprise Edge will wait between user-dialed digits. This value allows Enterprise Edge to determine when the user has stopped dialing. The value is programmed from the **Routing service** feature.

The user can also use the ‘#’ key to tell Enterprise Edge that they are finished dialing however, this is not usually required except for international calls where the number of digits dialed varies.

Under **Routing service, Dialing timeout**, select a different timeout value.

You can select one of the following values (in seconds): **3, 4, 5, 6, 8, 10, 15**. Too small a timeout value forces you to enter the digits very quickly one after the other, and too large a value causes the system to wait for a long time after the last digit is entered before the call is actually made.

For more information on non-PRI routing tables and destination codes, see Routing service on page 114.

Common settings

Services share the settings for control sets, schedule names and schedule times.

Control sets

A control set turns Services on and off for the lines and/or telephones assigned to it. You can assign several control sets for your system. A control set for lines controls Ringing service, Restriction service, and Routing service for its assigned lines; a control set for telephones controls Restriction service and Routing service for its assigned telephones. Assign a control set for each external line and telephone.

Enter the internal number of the control set for each line and for each set.

Tips

External lines and telephones must be programmed with a control set to use the three kinds of Services. You can assign a control set to more than one external line or telephone, but a line or telephone cannot be assigned to more than one control set.

One recommendation is to have one control set for all lines and a different control set for all telephones.

A service can be turned on manually or automatically for all external lines and telephones controlled by a given control set, but you cannot combine schedules. In other words, a service can only be active as normal service or one of the six schedules at any one time. You can have several schedules active, as long as they are using different services.

The default control set for all lines and telephones is 221.

Schedule names

The schedule name is shown on the display of the control set when the schedule is turned on. It identifies the active schedule. Enter a name of one to seven characters in the Name field at the top of the Unified Manager window.

Tips

The default names of the six possible schedules are only suggestions and may be changed to any other name. A schedule name can be one to seven characters long. It is recommended that you reserve certain schedules (4, 5, and 6) exclusively for alternate call routing (Routing service).

Schedule times

Schedule start and stop times are set at times you are most likely to want each service to be active.

Under **Common settings, Schedule times**, enter the start and stop times for each schedule, on each day.

Schedule	Start time	Stop time
Schedule 1: Night	23:00	07:00
Schedule 2: Evening	17:00	23:00
Schedule 3: Lunch	12:00	13:00
Schedule 4: Schedule 4	00:00	00:00
Schedule 5: Schedule 5	00:00	00:00
Schedule 6: Schedule 6	00:00	00:00

Tips

It is only necessary to program start and stop times for schedules that are activated automatically. See the instructions with Ringing service for information on activating schedules.

The time may be entered in either 12 or 24-hour format. If the display is in English, and the hour entered is less than thirteen, the display prompts you to specify **AM** or **PM**.

If you assign identical start and stop times for a schedule, for example, 04:00 start and 04:00 stop, the schedule is in effect all day. The only exception to this is a start and stop time of 00:00; in this case the schedule is off for the day.

You may assign overlapping times. For example, if schedule 1 is assigned from 9:00 am to 4:00 pm and schedule 2 is assigned from 1:00 pm to 5:00 pm, then the start time of the second schedule is treated as a stop time for the first schedule.

This is also true if two schedules have the same start time but different stop times; the stop time of the shorter schedule is treated as the start time of the longer schedule.

If one schedule starts and stops within the times of another schedule, the first service temporarily ends when the second service starts. The first service then resumes when the second service has ended.

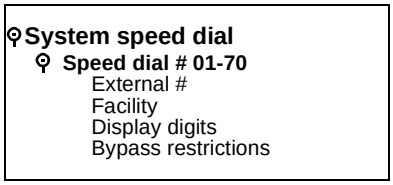
Some schedules start and stop at the same times each day: use **COPY** to copy the start and stop times from one day to the next.

Start and stop times don't span days.

When you program a schedule to start in the evening and stop in the morning, it does not carry over into the next day. For example, if you program Night service for Friday (22:00 to 6:00), the system turns on Night service from midnight to 6 am on Friday, and then again from 10 pm to midnight on Friday.

System speed dial

The System speed dial heading allows you to specify speed dial codes (01 - 70) and external numbers that can be used by any telephone set on the system. The following illustration shows a detailed view of the System speed dial programming map.



Adding or changing a system speed dial

You program a speed dial on your Enterprise Edge system so that anyone in your office can dial a frequently-used number using a two-digit code. Examples of system speed dials might include telephone numbers of regional sales offices within your organization or key customers that you call frequently.

To change a speed dial that already exists, follow the same steps as if you are creating a new system speed dial. The new programming overwrites the previous number and settings.

If you are creating a system speed dial for the first time you will need to choose the type of facility for the system speed dial. For more information about programming line facilities, see Line type on page 101.

The system has a standard name to display, so it is not necessary for you to program one; however, if you choose not to display the telephone number, you may want to create a more descriptive name.

To create a system speed dial:

1. Choose **Resources**, **Telephony**, **System Speed dial**.

2. Click a speed dial (Speed dial # 01 to 70).

3. In the **External #** box, type the telephone number (up to 24 digits) and press Enter.

   If this is a new speed dial, more fields appear after you press Enter.

4. Click a Facility value: **Use prime line**, **Use line:nnn**, **Pool code:x**, or **Use routing table**.

   where
   nnn is an integer between 001 and 238
   x is a letter between A and O

   Note: If you assign a specific line to a system speed dial number, only telephones with an appearance of that line can use the speed dial number.

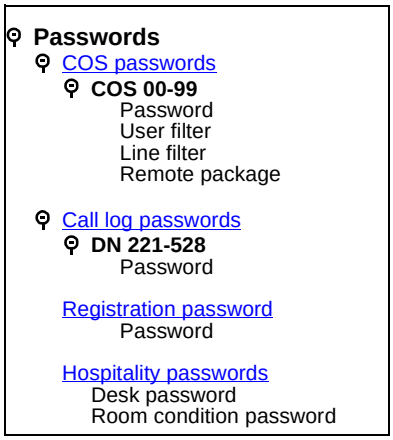
5. Click a Display digits value: **Y** (Yes) or **N** (No).

   Note: If you choose not to display the digits, the name of the Speed Dial code is displayed instead of the phone number. The default is Y.

6. Click a Bypass restrictions value: **Y** (Yes) or **N** (No).

Passwords

The Passwords heading allows you define class of service passwords, call log passwords, registration passwords (Companion wireless) and Hospitality passwords. The following illustration shows a detailed view of the Password programming map.



COS passwords

Class of Service (COS) passwords permit controlled access to a system's resources by both internal and remote users. When you enter a Class of Service password at a telephone, the restriction filters associated with your Class of Service password apply instead of the normal restriction filters. Similarly, when a remote user enters a Class of Service password on an incoming auto-answer line, the restriction filters and remote package associated with their Class of Service password apply instead of the normal restriction filters and remote package.

COS passwords lets you define individual passwords and determine the restriction filters and remote package associated with each.

Tips

The Class of Service passwords for a system should be determined randomly and should be changed on a regular basis.

Users should memorize their COS passwords instead of writing them down. Employees' COS passwords should be deleted when they leave the company. Typically, each user has a separate password. Alternately, several users can share a password or one user can have several passwords.

A system can have a maximum of 100 six-digit COS passwords (00 to 99).

You can copy the restriction filters and remote package from one COS password to another. COS passwords must be unique.

To assign a COS password:

1. Choose **Resources**, **Telephony**, **Passwords**, **COS passwords**.

2. Click a COS group (COS 00-99).

3. Type a 6-digit password in the Password box and press Enter.

4. Click a User filter value: **None** or **Filter:** . If **Filter:** is selected, type the 2-digit user filter and press Enter.

5. Click a Line filter value: **None** or **Filter:** . If **Filter:** is selected, type the 2-digit line filter and press Enter.

6. Click a Remote package value: **None** or **Package:** . If **Package:** is selected, type the 2-digit remote package and press Enter.

User filter

User filter lets you assign a restriction filter to a Class of Service password. The user filter associated with the Class of Service password replaces any normally applicable set restriction, line/set restriction, and remote restriction. The default setting (**None**), means that any normally applicable filters (set restriction, line/set restriction, or remote restriction) still apply.

Line filter

Line filter lets you assign a specific line restriction to a Class of Service password. The line filter associated with the Class of Service password replaces any normally applicable line restriction. The default setting (**None**), means that any normally applicable line filter still applies.

Remote package

Remote package lets you assign a specific remote access package to a Class of Service password. The remote access package associated with the Class of Service password replaces any normally applicable remote access package. The default setting (**None**), means that any normally applicable remote access package still applies.

Call log passwords

Call log passwords allows you to clear an individual's Call log password. This is useful if a user has forgotten the password and you need to reset it. Select the set DN and leave the field blank or enter a new password. The user can then enter a new password from their telephone.

To create or reset a call log password:

1. Choose **Resources**, **Telephony**, **Passwords**, **Call log passwords**.
2. Click a telephone set (DN 221-528).
3. Type a 4-digit password in the Password box and press Enter.

Registration password

To ensure unauthorized portables are not registered to your system, a separate level of password access is provided. You can, and should, set your own password to prevent unauthorized use. The default password is **RADIO** (72346).

To change the Registration password:

1. Choose **Resources**, **Telephony**, **Passwords**, **Registration password**.
2. Type a 5-digit password in the Password box and press Enter.

Hospitality passwords

The Hospitality Services feature allows for two types of passwords to access different areas of Hospitality programming.

Desk password

The Desk password is used to control access to all Hospitality Services administrative features. The default Desk password is **HOSP** (4677). It is recommended that you change the password to prevent unauthorized use.

To change the Desk password:

1. Choose **Resources**, **Telephony**, **Passwords**, **Hospitality passwords**.
2. Type a 1- to 6-digit password in the Room condition password box and press Enter.

Room condition password

The Room condition password controls access to the Room condition feature (Feature 8 7 6). The default Room condition password is **None**. For more information about using Feature 8 7 6, see the *Enterprise Edge Feature Telephone Programming Guide*.

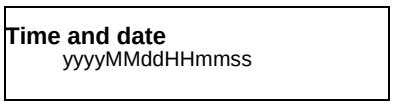
To create a Room condition password:

1. Choose **Resources**, **Telephony**, **Passwords**, **Hospitality passwords**.

2. Type a 1- to 6-digit password in the Room condition password box and press Enter.

Time and date

The Time and date heading allows you to change the system time and date. The following illustration shows a detailed view of the Time and date programming map.



You can configure the system to automatically change the time for Daylight savings. From Feature settings, enable **Daylight savings time**. For more information, see Feature settings **on page 136**.

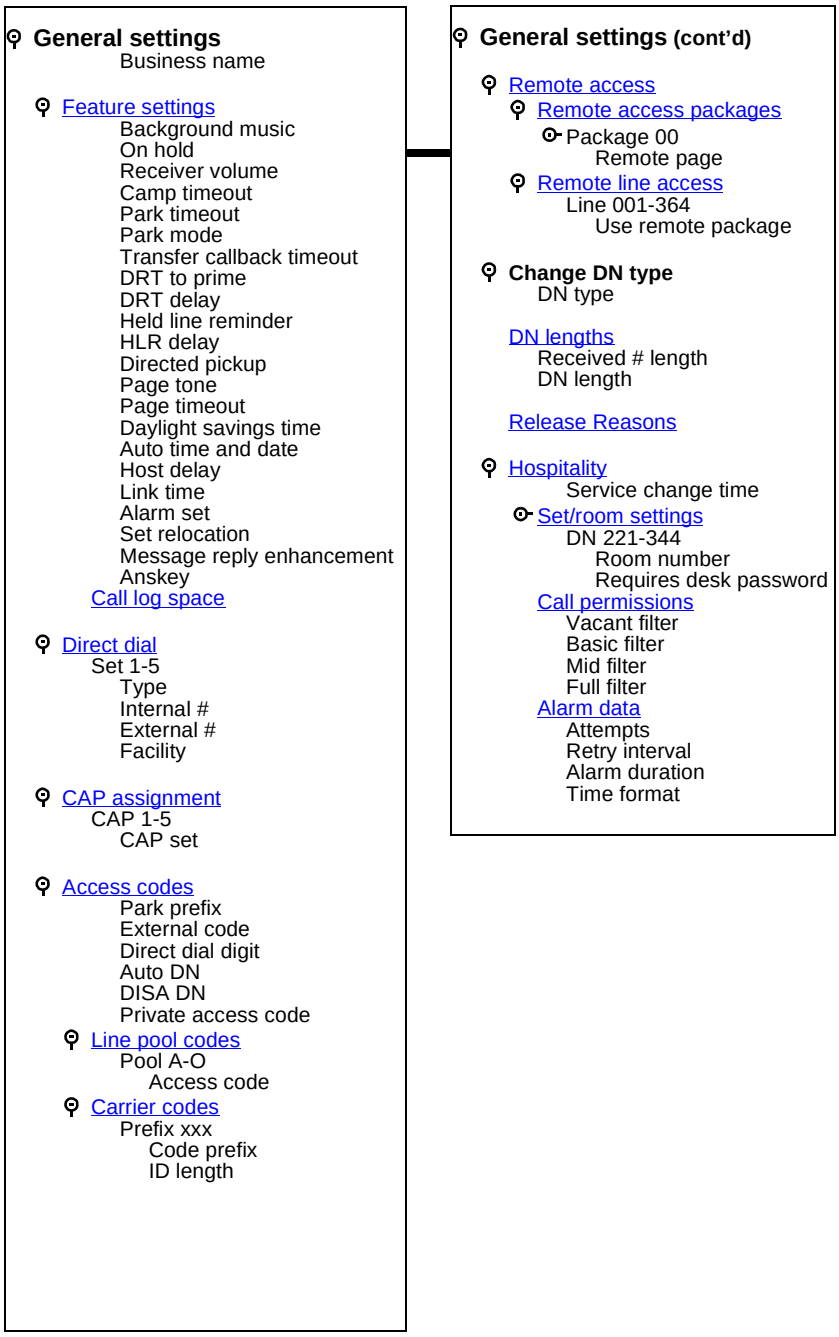
To change the time and date:

1. Choose **Resources**, **Telephony**, **Time and date**.

2. Type the time and date according to the format: yyyyMMddHHmmss and press Enter.

General settings

General settings heading allows you to define features and settings that are not associated with any specific line or telephone. The following illustration shows a detailed view of the General settings programming map.



Business name

Select General settings in the navigation list to view the **Business name** field in the Unified Manager window.

To change the business name:

1. Choose **Resources**, **Telephony**, **General settings**, **Feature settings**.

2. Type a name up to 7 characters and press Enter.

Change DNs

Change DNs allows you to change the directory number (DN) or internal number of a telephone in the Change DNs dialog box.

Changing DN locks programming session.
Changing an individual DN locks the programming session into the Change DNs programming mode. To unlock the programming session, exit and restart the Unified Manager.

On the Configuration menu, click Change DN. Enter the DN you want to change ("old DN"). Then, enter the new DN. Click **Change DNs** and **Save**.

Changing the starting DN number

You can change the starting number for your telephone directory numbers (DNs). This is helpful when your system is part of a network and you want to use a uniform series of directory numbers for all telephones in your network.

1. Enter the new directory number you want as the starting DN. The new range of DN numbers will be displayed. The length of the new DN can be from three to seven digits on all systems.

Feature settings

Feature settings allows you to program a number of features that are not associated with an individual telephone set. These settings apply to all telephones connected to the Enterprise Edge system.

To configure feature settings:

1. Choose **Resources**, **Telephony**, **General settings**, **Feature settings**.

2. Configure feature settings according to the table:

Attribute	Description
Background music	Allows you to listen to music through your telephone speaker. A music source must be connected to Enterprise Edge. Values: Y or N (Default: N)
On hold	Allows you to choose what a caller hears on an external line when the line has been put on hold. Tones provides a periodic tone. Music provides any signal from a source such as a radio connected to Enterprise Edge. Silence provides no audio feedback. Values: Tones, Music, Silence (Default: Tones)
Receiver volume	Allows you to specify whether the volume level of a receiver or headset will return to the system default level when a call is ended or put on hold, or whether it will remain at the level set at the individual telephone. Values: Use system volume, Use set volume (Default: Use system volume)
Camp timeout	Allows you to assign the number of seconds before an unanswered camped call is returned to the telephone which camped the call. Values: 30, 45, 60, 90,120, 150 or 180 seconds (Default: 45)
Park timeout	Allows you to assign the number of seconds before a parked call on an external line returns to the originating telephone. Values: 30, 45, 60, 90, 120, 150, 180, 300 or 600 seconds (Default: 60)
Park mode	Allows you to define how retrieval codes are assigned to parked calls. For more information, see page 139. Values: Lowest or Cycle (Default: Lowest)
Transfer callback timeout	Allows you to specify the number of rings before a callback occurs on a transferred call. You can estimate the delay in seconds if you multiply the number of rings by six. Values: 3, 4, 5, 6 or 12 (Default: 3)
DRT to prime	Defines whether or not unanswered external calls are automatically forwarded to a prime telephone after a certain period of time. For more information, see page 139. Values: Y or N (Default: Y)
DRT delay	Allows you to specify the number of rings before Delayed Ring Transfer transfers a call to a prime telephone. DRT to prime must be enabled before you can use this feature. You can estimate the delay in seconds if you multiply the number of rings by six. Values: 1,2,3,4,6 or 10 (Default: 4)
Held line reminder	Reminds you that a call at your telephone is still on hold. You periodically hear two tones from your telephone until you return to the call on hold. Values: Y or N (Default: N)
HLR delay	Allows you to choose the number of seconds before the Held line reminder feature begins at a telephone that has an external call on hold. Values: 30, 60, 90, 120, 150 or 180 (Default: 60)

Attribute	Description
Directed pickup	Directed pickup allows you to answer any calls by specifying the ringing telephone's internal number. For more information, see page 139. Values: Y or N (Default: Y)
Page tone	Defines whether or not a tone sounds before a page begins. Values: Y or N (Default: Y)
Page timeout	Defines the period of time after which the paging feature is automatically disconnected. Values: 15, 30, 60, 120, 180, 300, 600 2700 seconds (Default: 2700)
Daylight savings time	Defines whether or not the clock on the MSC automatically switches between standard time and daylight savings time. For more information, see page 139. Values: Y or N (Default: Y)
Auto time & date	Defines whether or not the system to automatically updates the time and date after a power failure. For more information, see page 140. Values: Y or N (Default: Y)
Host delay	Assigns the delay between the moment an outgoing line is selected to make an external call (for example, by lifting the receiver off the telephone) and the moment that Enterprise Edge sends dialed digits or codes on the line.This ensures that a dial tone is present before the dialing sequence is sent. Minimizing this delay provides faster access to the requested features. Values: 200, 400, 600, 800, 1000, 1200, 1400, 1600, 1800 or 2000 milliseconds (Default: 1000)
Link time	Allows you to specify the duration of a signal required to access a feature through a remote system. For more information, see page 140. Values: 100, 200, 300, 400, 500, 600, 700, 800, 900 or 1000 milliseconds (Default: 600)
Alarm set	Alarm set allows you to assign a telephone on which alarm messages appear when a problem has been detected in the system. Alarms are recorded in the Windows NT™ event log. Values: None, DN: (Default: 221)
Set relocation	Allows you to move any telephone to a new location within the Enterprise Edge system without losing the directory number, autodial settings, personal speed dial codes, and any programming for that telephone. For more information, see page 140. Values: Y or N (Default: N)
Message reply enhancement	Activates the Message reply enhancement feature. For more information, see page 141. Values: Y or N (Default: Y)
Answer key	Allows you to determine what types of calls will alert at the telephone. For more information, see page 141. Values: Basic, Enhanced, or Extended (Default: Basic)

Park mode

The Call Park feature lets you suspend a call and lets someone retrieve the call by entering a retrieval code at any Enterprise Edge set in the system. Park Mode is the setting which determines how a retrieval code is assigned to parked calls.

Select the way that the system will choose a Call Park code: **Lowest** or **Cycle**.

When set to Lowest, the system will choose the lowest code that is available when the call is parked. When set to Cycle, the system will choose the codes in a sequence, from lowest to highest, until all the codes have been used.

DRT to prime

Delayed Ring Transfer automatically forwards unanswered external calls to a prime telephone, after a certain period of time. This helps ensure that no external call goes unanswered.

Tips

An operational prime telephone must be assigned before this feature can operate. A prime telephone is assigned to one or more external lines in the Line Data of programming.

Directed pickup

Directed pickup allows you to answer any calls by specifying the ringing telephone's internal number.

Tips

Directed pickup is not to be confused with the Call Pickup Group feature in programming, which allows you to answer a call at any telephone within a specific group without specifying the internal number of the ringing telephone.

Like Call Pickup Group, Directed pickup is useful when not all the telephones have been assigned the same lines, but you still want to allow your co-workers to answer a call on any external line from their telephones.

Daylight savings time

When this feature is turned on, the clock on the MSC will automatically switch between standard time and daylight savings time.

Tips

The hour falls back one hour on the last Sunday of October at 2:00 am., and it advances one hour on the first Sunday of April at 2:00 am.

In regions where daylight savings time does not apply, (for example, Saskatchewan), make sure this setting is disabled).

Auto time & date

You can program the Automatic time and date feature for the clock on the MSC to enable the Enterprise Edge system to automatically update the time and date after a power failure.

Whenever the clock is out of sync by more than two minutes as a result of a power failure or a loss of power, the first incoming call updates the clock automatically after two rings.

Note: CLASS trunks are required for this feature to work. Consult your customer service representative to determine if you have CLASS trunks.

This feature also allows the automatic changing between North American daylight savings and standard time. The Automatic Time and Date feature automatically overrides any manually programmed changes to the time and date in your system.

Note: The year is not included with the time and date information and must be programmed manually if the current year differs from the network time.

Click **Y** or **N** to enable Automatic time & date.

Link time

Link time allows you to specify the duration of a signal required to access a feature through a remote system.

For example, to program external dialing through a Centrex system, which requires a Link time of 400 ms, specify a Link time of 400.

Tips

The Link time required depends on the requirements of the host switching system that must be accessed.

Link is another name for recall or flash.

Set relocation

Set relocation allows you to move any telephone to a new location within the Enterprise Edge system without losing the directory number, autodial settings, personal speed dial codes, and any programming for that telephone.

Tips

It is advisable to activate Set relocation after the set installation and programming has been done. This provides you with more flexibility in testing equipment.

If this feature is deactivated while a set is moved, that set's internal number and programming data remain with the physical port on Enterprise Edge, and the set does not receive the original programming when it is reconnected elsewhere.

Message reply enhancement

The Message reply enhancement feature allows for the message waiting indicator on analog telephones connected to an Enterprise Edge Analog Station Media Bay Module (EE-ASM) to be deactivated automatically if the reply call from the analog telephone to the designated direct-dial telephone is answered, no matter where the call is answered from by the user.

This feature also functions if the user invokes the Call Pickup feature to answer the reply call from the analog set. It does not however, work with the Retrieve Parked Call feature.

Tips

Direct-dial sets are the only sets that can send messages (using Feature 1) to analog telephones connected to an Enterprise Edge Analog Station Media Bay Module (EE-ASM). The direct-dial set must be the designated direct-dial set for the analog telephone receiving a message.

Answer key

There are up to eight answer keys that can be assigned per set. The Answer key setting in Feature settings programming lets you determine what types of calls will alert at the telephone. Answer key changes do not apply to portables.

Your choices are: **Basic**, **Enhanced** and **Extended**.

With the default Basic setting, answer keys do not ring for:

- Prime set call capture
- call forwarded calls
- other answer key calls
- priority calls
- voice calls
- ringing service
- callbacks

The Enhanced setting is the same as the Basic setting except that answer keys will ring for overflow call routed calls (special case of Prime set call capture). Answer keys will not ring for line transferred calls (although Basic will ring).

Extended will ring for all call types except priority calls and voice calls.

Select the setting: **Basic**, **Enhanced**, and **Extended**.

A Phantom DN is a line that can be programmed to appear and ring on a set that does not physically exist. It allows you to create an Answer Key for the set that does not exist.

Call log space

Call log space programming customizes how log space is allocated to telephones in the system. Reset logs allows you to reallocate the Call log space equally to all telephones in your system.

To Reset logs:

1. On the Configuration menu, click **Reset logs**.
2. Enter the space allocation for the Call log at each telephone. You must use a three-digit number (for example, 020 to give each set 20 spaces).
3. Enter the number of sets with logs.
4. Click **OK**.
5. The system automatically reallocates Log space. Select **NO** to keep existing settings.

Tips

Use this heading only if you want to allocate an equal amount of log space to all the telephones in your system.

Reallocating Call log space may destroy Call log data at telephones that lose space.]

There are 600 Call log spaces available in the system. There are no spaces allocated by default. Changing the space allocation using Log Defaults defines the log space available to all telephones in the system. Any remaining unassigned log space is available in a log pool, and can be reallocated from **Terminals & Sets**/ **Telco features**.

Direct dial

Direct-dial lets you dial a single system-wide digit that can be used to call a specific telephone, called a direct-dial telephone. The most common example of a direct-dial set would be telephone for an operator, a receptionist or an attendant.

Set 1 - Set 5

For the direct-dial set, indicate whether it has an internal or external number. A total of five direct-dial sets can be programmed on the system.

Select the setting: **Internal**, **External**, or **None**.

Internal / External#

Enter the internal or external number that the system will automatically dial when someone enters the direct-dial digit. The default number for the direct dial set is **221**.

Facility

If you assign an external number as a direct dial set, you must indicate which line to use for the call. Select the line for the external number: **Pool A** to **O**.

Tips
There is just one direct-dial digit for the entire system. The Enterprise Edge system cannot verify that the number you assign as an external direct-dial set is valid. Check the number before assigning it as a direct-dial set, and call the direct-dial set after you've assigned it in order to test it.

CAP assignment

This setting designates a telephone as a central answering position (CAP). The CAP must be an M7324 telephone, and may have one or two CAP modules attached. A maximum of five CAPs can be installed in an Enterprise Edge system.

The CAP may be used to:

- monitor the busy/not busy and Do Not Disturb status of Enterprise Edge telephones
- answer external calls on up to 120 lines, and extend calls to other Enterprise Edge telephones
- send up to 30 messages to other Enterprise Edge telephones
- provide up to 96 extra memory buttons for the M7324 telephone

Under **CAP assignment, CAP1, CAP set**, enter the internal number of the M7324 telephone to be designated a CAP.

Tips
If CAP modules are attached to an M7324 telephone that has not been programmed as a CAP, then no CAP settings are assigned. If a CAP module (or modules) is relocated with the M7324 telephone, the settings are retained.

Access codes

Access codes are used by the system to direct calls to the correct lines and destinations. If the codes conflict, some of the features on the system will not work.

The table of default settings can help you plan your access codes so there are no conflicts.

Digit	Use	Heading
0	direct-dial digit	Access Codes
1	Park prefix	Access Codes
2	the first digit of B1 DNs	Startup
9	line pool A access code (Takes precedence over the External Line access code if there is a conflict.)	Access Codes
— —	external line access code	Access Codes
— —	destination code	Services

Double click on **Access codes** to view settings in the Unified Manager window.

Park prefix

The Park prefix is the first digit of the call park retrieval code that must be entered to retrieve a parked call. If the Park prefix is set to None, calls cannot be parked. Select the setting: **None**, or **1**, **7, 8**.

Tips

The Park prefix cannot be the same as: the Direct-dial digit, the External Line access code, the first digit of a DN, the first digit of a line pool access code, or the first digit of a destination code.

Other programmable settings may affect which numbers appear on the window during programming. Although the numbers 0 to 9 are valid Park prefix settings, some may have been already assigned elsewhere by default or by programming changes. (To avoid a conflict, refer to the table of default settings in the description of External code.)

If DN length is changed, and the changed DNs conflict with the Park prefix, the setting changes to None.

External code

External code allows you to assign the external line access code. This code is used to allow M7100 telephones and Enterprise Edge ATA 2 to access external lines.

Select the setting: **None,** or **7, 8, 9**.

Tips

The external line access code cannot conflict with: the Park prefix, the direct-dial digit, the first digit of a line pool access code, the first digit of a DN, or the first digit of a destination code.

If DN range, and the changed DNs conflict with the external line access code, the setting changes to None.

Direct dial digit

Direct dial digit allows you to dial a single system-wide digit that can be used to call a specific telephone, called a direct-dial telephone.

Select the setting: **None**, or **0, 7, 8**.

Tips

Another direct dial telephone, an extra dial telephone, can be assigned for each schedule in Services programming.

The direct dial digit cannot be the same as the first digit of a DN, of a line pool access code, the external line access code or the Call Park prefix. It cannot be the first digit of a destination code.

If DN length is changed, and the changed DNs conflict with the direct dial digit, the setting changes to None.

Auto DN

For calls answered without DISA, no password is required to access the Enterprise Edge system. The Class of Service (COS) that applies to the call is determined by the COS for the trunk on which the user is calling. Enter the digits to be received from the auto-answer trunk.

Tips

The length of the Auto DN is the same as the Received number length specified in **General settings**.The Auto DN is cleared if the Received number length is changed.

The Auto DN cannot be the same as a line pool access code or a destination code.

DISA DN

For calls answered with DISA, the system presents a stuttered dial tone to prompt a caller to enter a valid password. The Class of Service (COS) that applies to the call is determined by this COS password.

Once a remote user is on the Enterprise Edge system, the DISA DN can be used to change the existing Class of Service. This gives you greater flexibility when you create access privileges. For example, you may want to have a shared DN for remote access and separate COS passwords with different dialing out privileges for individuals.

Enter the digits to be received from the auto-answer trunk.

Tips

The length of the DISA DN is the same as the Received number length specified in **General settings**. The DISA DN is cleared if the Received number length is changed.

The DISA DN cannot be the same as a line pool access code or a destination code.

Private access code

The Private access code is the first digit the user dials to access private facilities. It provides access to tandem and toll bypass functionality. For example, a PSTN user in Toronto could call a PSTN user in Ottawa and have the call routed over the private network connection from the Toronto office to Ottawa office and then out to the PSTN from the Ottawa office. This would bypass any long distance toll charges. To add this functionality, the destination code has to include the private access number. For an example of a toll bypass network configuration and its associated programming, see Toll bypass with Enterprise Edge VoIP Gateway on page 325.

The private access code can be up to two digits in length.

Line pool codes

This setting allows you to assign a line pool access code for each of the fifteen line pools (A to O). These codes are used to specify the line pool you want to use for making an outgoing external call. Enter the access code. The default access code is **9** for **Line Pool A**, for **Line Pool B** to **O**. No default is specified for Line Pools B to O.

For PRI, see Line Pools on page 155.

Tips

The code can be one to four digits in length.

A line pool access code can be the same as an external line access code. In this case, the line pool access code takes priority over the external line access code, and a line from the line pool is selected.

A line pool access code cannot conflict with: the Park prefix, the Direct-dial digit; the first digit of any Received number; the first digit of any DN (including the Auto DN or the DISA DN).

To avoid a conflict, refer to the table of default settings in the description of External code.

Carrier codes

For information on Carrier codes and their use, see page 124.

Remote access

Remote access packages allow you to control the remote use of Enterprise Edge line pools. Create a remote access package by defining which of your system's line pools it will be able to access. You then assign the package to individual lines (using Remote line access), and to a particular Class of Service password (Remote package in COS passwords).

Remote access packages

Select the remote access package you want to program.

LinePool access

Select Line Pool access and click **Add**. Enter a line pool code and click **Save**.

Remote page

Click **Y** or **N** to enable remote paging for each pool.

Remote line access

Select the line number of the line which will be accessible by remote users.

Use Remote package

Enter the number of the remote access package that will apply to remote use of the line.

Parameter	PBX DID
Package 00	Prohibits remote access to line pools, Page, remote monitoring and administration. Cannot be changed.
Package 01 Line pool access	 Y for Pool A N for Pools B to O and PRI-A to PRI-F
Packages 02 - 15 Line pool access	 N for Pools A to O and PRI-A to PRI-F

Tips

You can copy settings from one remote package to another.

The line pool access display shows an alphabetic line pool identifier, followed by a numeric line pool access code in brackets, for example, **Pool A (9):N**. If no access code has been identified, there is nothing between the brackets, for example **Pool A ( ):N**. The line pool access code can be programmed under **Terminals & Sets**.

Remote package 00 is the default setting for the Remote package setting. It permits no access to line pools. Unlike packages 01 to 15, package 00 cannot be changed.

You can define up to 15 remote access packages (01 to 15).

DN lengths

Received number length

The Received number length setting allows you to change the number of digits received on auto-answer trunks. These digits are used to identify target lines, Auto DNs, and DISA DNs. Select the setting: **2, 3, 4, 5, 6**, or **7**.

Tips

The target line number (for example, line 241) and the Received number for the target line (for example, **Received number: 123** for line 241) are two different numbers.

The Received number length may be the same as the system DN length, or may, because of network or central office constraints, be set to some other value.

Changing the Received number length causes all programmed received digits to be cleared.

DN length

This feature allows you to change the number of digits for all DNs. The maximum length is seven. The default and minimum length is **3**.

1. Select the setting: **3, 4, 5, 6**, or **7**.

   You will be prompted, "If NNV Message is installed, all messages and mailboxes will be deleted."

2. Select **OK** to save the new DN length. **Cancel** restores the original value.

Do not change DN length immediately after a system startup.

You must wait for at least two minutes after a system startup before you change the DN length.

Data devices drop calls when the DN length is changed. (These data devices use the B2 channel. The M7100, M7310, and M7324 telephones use the B1 channel. Calls are **not** dropped for these telephones.)

The DN length change is completed within two minutes, depending on the size of the installed Enterprise Edge system. System response may briefly slow down during this time.

Tips

A DN length change, if required, should be the first programming change on a newly installed Enterprise Edge system.

Each increase in length places the digit 2 in front of any existing DN. For example, if DN 234 was increased to a length of 4, the new DN would be 2234.

If the DN length is changed so that a conflict is created with the Park prefix, external line access code, direct-dial digit, or any line pool access code, the setting for the prefix or code is changed to None, and the corresponding feature is disabled.

Network Name Display

Enterprise Edge will display the name of the calling party when it is provided both Private or Public ISDN PRI interfaces. The displayed name may include information such as the Receiving Calling Name, Receiving Redirected Name, and/or Receiving Connected Name. The outgoing name is the business name concatenated with the set name. For information on programming your CLASS assignment, see Feature assignment on page 93.

Note: Network Name Display is an optional feature that is available based on the interface to which you are subscribed.

Feature	Interface		
	NI PRI	DMS Custom PRI	SL-1 (Premium telephony)
Receiving Calling Name	Supported	Supported	Supported
Receiving Redirected Name	Supported		
Receiving Connected Name		Supported	Supported
Sending Calling Party Name	Supported	Supported	Supported
Sending Connected Name		Supported	Supported

Receiving and Sending Calling Party Name

Network name display allows the name of an incoming PRI call to be displayed on the Enterprise Edge set receiving the call.

Calling Party Name with status of 'PRIVATE' may be displayed on the Called Party set as '**Private name**'. If the incoming Calling Name is defined by the CO as a private name, then '**Private name**' appears on the answering set. If the Calling Party Name is unavailable it may be displayed on the Called Party set as '**Unknown name**'.

The system supports sending the calling party name (Business Name and Set Name concatenated together) on calls originated by the Enterprise Edge system.

For information on programming your CLASS assignment, see Feature assignment on page 93. The Set Name will only be sent if the OLI for the Set is configured. See OLI # on page 83.

Receiving Redirected Name

Network name display allows the receiving of the Originally Called Name (Redirecting Name) on incoming calls. The Originally Called Name will be stored, but not displayed.

Receiving and Sending Connected Name

Network name display supports the reception of Connected Name on outgoing calls. The Connected Name is stored and displayed on the Enterprise Edge set.

In order for this to work you need to set the Called ID to yes. See Auto called ID on page 93.

The system also supports sending the Connected Name (Business and Set Name concatenated together) on incoming calls.

If the call is answered by a hunt group, the hunt group name is used instead of the set name in forming the connected name.

The Connected Name is a transient display that appears for about 3 seconds.

Network Name Display interactions

Calling and Connected Name information (if available) is passed between trunks with Selective Line Redirection (SLR). Only Calling Name information is passed between trunks in cases where Direct System Inward Access (DISA) has resulted in tandeming of trunks.

Programming Network Name Display

The Business Name and the Set Name make up the information that is used for the outgoing Calling name or connected name.

Calling/connected name is only sent once the Business Name is programmed. To program the Business Name use **Hunt groups, BusName**.

Enter a Business Name. You can enter a maximum of eight letters. It is recommended that you use a blank space for the last character to act as a separator between the Business name and Set name.

To program the Set Name:

1. Under **Terminals & Sets,** select the set number of the telephone
2. Under **Line access, Name**, enter a maximum of seven letters.

3. Other areas that must also be programmed include:

   - the OLI number, see OLI # on page 83
   - under Telco features the Call ID must be set to yes, see Auto called ID on page 93
   - under lines you need to enter the set number where you want the CLID to appear, see CLID set on page 102

Outgoing Name and Number Blocking

When activated, Feature 8 1 9 blocks the outgoing name and number (ONN) on a per call basis. When this feature is used, the call is flagged to the CO so that the name and number will not be presented to the person being called.

The CO is alerted by two methods and each depends on the type of trunk involved in placing the outgoing call. Analog trunks use a dialing digit sequence called a Vertical Service Code (VSC). The VSC differs from region to region and must be programmed. Analog trunks with both tone and pulse dialing trunks can have separate VSCs. PRI trunks have only one VSC.

To configure ONN:

1. Select **Telco Features**.
2. For analog trunks under **Voice Message center numbers, ONN Blocking, Analog VCS, Tone:None.** You can choose F78, (0-9), *, #.
3. Enter a new tone dialing Name and Number blocking digit sequence.
4. For non-analog trunks under **Voice Message center numbers, ONN Blocking,Pulse:None.** You can choose F78, (0-9), *, #.
5. Enter a new pulse dialing Name and Number blocking digit sequence.

Call by Call service selection for PRI

Call by Call service selection allows a user to access services or private facilities over a PRI line without the need for dedicated facilities. The different services represent different types of access to the network. Various services (see list below) are available depending on the chosen protocol.

Call by Call service selection is supported for the following protocols:

- National ISDN 2 (NI-2)
- DMS-100 custom
- DMS-250 (MCI, Sprint, Generic)
- AT&T 4ESS custom

The following Call by Call Services are supported:

- Public
- Public calls connect Enterprise Edge and a Central Office (CO). Both incoming (DID) and outgoing (DOD) calls are supported. Dialed digits conform to the standard North American dialing plan (E.164 standard).
- Foreign Exchange (FX)

  Foreign exchange service connects an Enterprise Edge site to a remote central office (CO). This provides the equivalent of local service at the remote location.
- Tie

  Tie lines are private incoming and outgoing lines that connect Private Branch Exchanges (PBXs) such as Enterprise Edge.
- Outward Wide Area Telecommunications (OUTWATS)

  This outgoing call service allows an Enterprise Edge user to call telephones in a specific geographical area referred to as a zone or band. Typically a flat monthly fee is charged for this service.
- Inward Wide Area Telecommunications (INWATS)

  This long distance service allows an Enterprise Edge user to receive calls originating from specified areas without charge to the caller. A toll-free number is assigned to permit reverse billing.
- International INWATS

  An international long distance service that allows an Enterprise Edge user to receive international calls originating from specified areas without charge to the caller. A toll-free number is assigned to permit reverse billing.
- Switched Digital

  This service provides premises to premises voice and data transport with call management and monitoring features.
- Nine Hundred

  This service is commonly referred to as fixed charge dialing.
- Private

  Private incoming and outgoing calls connect Enterprise Edge to a virtual private network. Dialed digits may conform to the standard North American dialing plan (E.164 standard) or the dialed digits may use a private dialing plan.

NNV Service[a]	NI-2[f]	DMS-100 (custom)	DMS-250 (MCI, Sprint, Generic)	AT&T 4ESS
FX	FX	FX[b]		
Tie[c]	Tie	Tie	Tie	SDN (software defined network)
INWATS	INWATS	INWATS	Eight Hundred	Toll Free MEGACOM
International INWATS	Same as INWATS	Same as INWATS	Same as INWATS	International Toll Free Service
OUTWATS	IntraLATA OUTWATS OUTWATS with bands InterLATA OUTWATS	OUTWATS	PRISM	MEGACOM
Private		DMS Private[e]	VNET (virtual network)	
Switched Digital				ACCUNET[d]
Nine Hundred			Nine Hundred	MultiQuest
Public	Public	Public	Public	

a. A shaded box indicates that the protocol does not support the service.
b. DMS-250 Sprint and UCS support incoming FX only (i.e. Network-to-Enterprise Edge). DMS-250 MCI does not support FX.
c. NI-2 allows two Tie operating modes: senderized and cut-through. Enterprise Edge will only support senderized mode.
d. Rates greater than 64 kbps will not be supported.
e. Bell Canada VNET.
f. Not all service types may be supported by a switch type. For information, contact your service provider.

Programming Call by Call on PRI requires you to program various areas of the Enterprise Edge system such as

- under **Line access**, assign the line pool
- under **Services**, in routing services section, assign which pool to use for routing and which service type, and service id if required
- under **General settings**, specify the minimum and maximum values for the pools
- under **Hardware** choose DTI (PRI) and select the protocol

Programming Call by Call service selection

Programming the Enterprise Edge system for Call by Call Service Selection with a PRI interface requires

- provisioning a DTI as PRI if a DTI configured as PRI is not already a part of the system, see the Maintenance section
- selecting a protocol, on page 178
- programming incoming call routing, on page 180
- programming routes that use the PRI pools (under Services), see Routing service on page 114

PRI Call by Call Limits

PRI pool limits for Call by Call services allows you to configure limits for service types without interacting with the CO. This feature sets the minimum and maximum number of incoming and outgoing calls per service type for the PRI pool.

The number of active calls will be tracked and whenever a call is being setup, a check will be made to determine if it will be allowed. Calls will not be allowed if they exceed the maximum value for that service type or if they will use lines needed to maintain the minimum value of other service types.

The summation of the minimum values for incoming or outgoing PRI services cannot exceed the total number of lines in the PRI pool.

The maximum value for an incoming or outgoing PRI service cannot exceed the total number of lines in the PRI pool.

Programming Call by Call Limits

1. From **General settings, Call by Call limits**, select a pool (PRI-A to PRI-F) that supports Call by Call routing.

2. Select a service under **Service:**.
   The service that is displayed depends upon the protocol.

3. Enter a number if required under **Min incoming:2**.

4. Enter a number if required under **Max incoming:23**.

5. Enter a number if required under **Min outgoing:4**.

6. Enter a number if required under **Max outgoing:23**.

Release Reasons

This feature is useful for diagnostic purposes. It shows the reason why an ISDN call has been released. The Release Reason can be displayed as Simple or Detailed text. When the default **None** is selected, no release reasons appears on the set.

1. Select **General settings, Release reasons.**

2. Choose a Text setting: **Simple**, **Detailed,** or **None.**

Note: If you selected Simple text the **Cause code** must be disabled. This is for diagnostics.

Line Pools

All lines in a PRI interface are in the same PRI line pool. This pool cannot contain any non-PRI lines. There is one PRI pool available for each PRI interface. Depending on the order that the modules are configured as PRI, Pool PRI-A represents lines 061 to 083, Pool PRI-B represents lines 085 to 107, and Pool PRI-C represents lines 109 to 131, etc. to Pool PRI-F. If all PRIs are connected to the same service provider and use the same protocol, lines 061 to 083, 085 to 107, and 109 to 1311 etc. can be put in the same pool, PRI-A, PRI-B, PRI-C up to PRI-F.

Hospitality

Hospitality Services (HS) is a group of features that increases the value of the Enterprise Edge system in small- to medium-sized facilities such as hotels, motels or hospitals.

In a hotel setting, guests gain improved services through immediate access to basic functions like:

- wake-up service or reminders
- accurate tracking of the room's service requirements.

Enterprise Edge telephones are classified as one of three types of sets: a common set, a room set or a Hospitality Services (HS) admin set.

Common set

A common set can be a telephone found in a lobby, office, or common area. It is not associated with a room and does not have access to all of the HS features.

Common sets are Enterprise Edge telephones or analog telephones connected to an analog terminal adapter (ATA), or an analog station module (ASM).

Room set

A Room set is a set assigned to a room. Up to five sets can be assigned to the same room (they all share same room number).

Room sets can be any Enterprise Edge telephone or an analog telephone connected to an ATA or an ASM.

Hospitality Services (HS) admin set

A Hospitality Services (HS) admin set is any two-line display Enterprise Edge telephone. An HS admin set can be programmed to require a user to enter the Desk admin password before access to HS administrative features is granted.

Alarm time (AL) feature

The Alarm time feature provides an alarm clock capability on Enterprise Edge and analog telephones connected to an ATA or an ASM. Both room sets and common sets can be programmed to sound an audible alert at a requested time.

One Alarm time within a 24 hour period is programmable on a room or common set and must be reset daily. When the alarm sounds, all sets in a given room alert. Canceling the alarm on any set cancels the alarm on all the sets in the room. A new Alarm time entered on a room or common set overwrites any alarm set previously.

If the Enterprise Edge system experiences a power failure, the failure can result in missed Alarm times. When the Enterprise Edge system is running and the system's time resets, the missed Alarm times alert in respective room or common sets. At all times, the Enterprise Edge system allows up to a maximum of 25 sets that can alert at the same time.

For more information about programming this feature, see the *Enterprise Edge Feature Telephone Programming Guide*.

Service time

The Hospitality heading allows you to enter the time when occupied rooms change state from Service done to Service required. The Service change time is an integral part of the Room condition (RC) feature.

To change the service time:

1. Choose **Resources**, **Telephony**, **General Settings**, **Hospitality**.

2. Type the time in the Service change time box according to the following format press Enter:

   hh is a number from 00 to 23
   mm is a number from 00 to 59

Set/room settings

The Set/room settings heading allows you to assign sets to a room and enable access control to HS administrative features.

To assign a set to a room:

1. Choose **Resources**, **Telephony**, **General Settings**, **Hospitality**, **Set/room settings**.

2. Click a DN number (DN 221-344).

3. Type a room number in the Room number box and press Enter.

To enable or disable password control:

1. Choose **Resources**, **Telephony**, **General Settings**, **Hospitality**, **Set/room settings**.

2. Click a DN number (DN 221-344).

3. Click a Requires desk password value: **Y** or **N** and press Enter.

   The default setting is **Y**. This means that administrative features cannot be accessed from a room set without first entering a valid password. The Hospitality passwords heading is used to define a Desk password. For more information, see Desk password on page 132.

Call permissions

The Call permissions heading allows you to assign dialing filters to room sets based on the room occupancy status. The Vacant state indicates that the room is empty. The Basic, Mid and Full states indicate that the room is occupied. The default dialing filter for all Room occupancy states (Vacant, Basic, Mid, and Full) is **00**. The dialing filters are standard the Restriction filters used in Enterprise Edge (Filters 00-99). For more information, see Restriction filters on page 108.

To assign dialing filters:

1. Choose **Resources**, **Telephony**, **General settings**, **Hospitality**, **Call permissions**.

2. Type a 2-digit filter number in the Vacant, Basic, Mid or Full box and press Enter.

Alarm data

The Alarm data heading allows you to program the following alarm settings:

- Attempts - The number of times the Alarm time feature attempts to alert the occupant before cancelling.
- Retry interval - The interval period in minutes between each attempt.
- Alarm duration - The period in seconds for which a set alerts for each alarm attempt.
- Time format - The hour format to be used, 12-hour or 24-hour.

To define the alarm data:

1. Choose **Resources**, **Telephony**, **General settings**, **Hospitality**, **Alarm data.**
2. Click an Attempts value: **1** to **5** and press Enter.

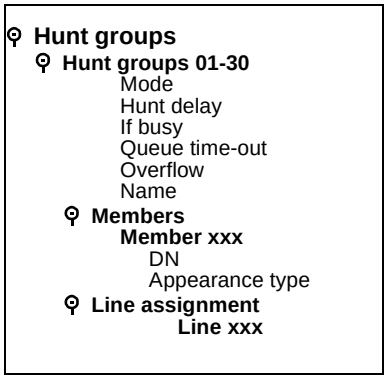
   The default value is **3** attempts.
3. Click a Retry interval value: **2** to **9** and press Enter.

   The default value is **4** minutes.
4. Click an Alarm duration value: **10**, **15**, **20**, **25**, **30**, **35**, **40**, **45** or **50** and press Enter.

   The default value is **15** seconds.
5. Click a Time format: **12 hour** or **24 hour** and press Enter.

Hunt groups

The Hunt Groups heading allows a group of Enterprise Edge sets to be called by a single directory number ensuring that calls are easily routed to the appropriate group. The following illustration shows a detailed view of the Hunt groups programming map.



Hunt Groups are used in situations where a group of people performing the same task are required to answer a number of related phone queries. Some typical uses of Hunt Groups are:

- a sales department answering questions on product prices or availability
- a support department answering questions concerning the operation of a product
- an emergency department answering calls for help.

Hunt Groups can be used to route calls to a support service such as a Help Line for a software company. Specialists dealing with Product A can be in one group, and specialists dealing with Product B can be in another group. Incoming calls hunt for the next available set in the group. If no set is available, the call can be placed in a queue or routed to an overflow set.

The Hunt Groups subheading in Resources, Telephony is the area where programming changes are made to the following:

- members of a group
- member position in a group
- what lines are assigned to a group
- how incoming calls are distributed
- how long the system looks for available members
- where a call goes if all members are busy

Note: Videophones should not be programmed as members of a Hunt Group. Hunt Groups allow one B channel connection at a time and videophones use two B channels.

The operation of some features varies if the Enterprise Edge set is part of a Hunt group. Features affected are summarized in the table below.

Feature	Description
Call Forward all calls	The Call Forward all calls feature is ignored and the Hunt group call rings at the set.
Call Forward no answer	The Call Forward no answer is ignored and the Hunt group call continues to ring until the hunt time has expired.
Call Forward on busy	The Call Forward on busy is ignored and the Hunt group call continues to ring until the hunt time has expired.
Do not Disturb on Busy	If this feature is active, the set will not receive notification of incoming Hunt group calls.
Group Pickup	If a set is part of a Hunt group and a call pickup group, then an incoming Hunt group call can be picked up from any set that is in the call pickup group.
Transfer via Hold	Transfer is supported on Hunt group sets; however, Transfer via Hold is not. Once a call is answered on a Hunt group set, its appearance disappears from all others sets in the Hunt group so that other calls can come in on the same line.
Priority Call	Priority calls cannot be made to Hunt group DNs.
Ring Again	Ring Again cannot be used when calling a Hunt group DN.
Line Redirection	The Allow redirect attribute should be set to N for lines assigned to Hunt groups. For more information, see Capabilities on page 86.
Page Zones	Hunt group DNs cannot be included in a Page zone.
Voice Call	Hunt groups cannot accept voice calls. Answer buttons have no appearances for voice calls, and the set does not ring.

Adding or removing members from a group

Members of the group can be any Enterprise Edge set, or portable. An Enterprise Edge set can be in more than one Hunt Group but is considered a member in each Hunt Group, increasing the total number of members in the system.

There can be only one appearance of the same Hunt Group on a set. Hunt Group DNs cannot be members of other Hunt Groups. A DN can be associated with a member of a Hunt Group and is called a member DN.

Consult your customer service representative to determine your Hunt Group number range.

To add a member to a hunt group:

1. Choose **Resources, Telephony, Hunt Groups**.

2. Click a hunt group (Hunt group 1-30).

3. Expand the hunt group and click **Members**.
4. Click the **Add** button.
5. Type a number in the DN number box.
6. Click the **Save** button.

To remove a member from a hunt group:

1. Choose **Resources, Telephony**, **Hunt Groups**.
2. Click a hunt group (Hunt group 1-30).
3. Expand the hunt group and click **Members**.
4. Click the member (for example, Member 001) to be removed.
5. Click the **Delete** button.

To remove all members from a hunt group:

1. Choose **Resources, Telephony**, **Hunt Groups**.
2. Click a hunt group (Hunt group 1-30).
3. Expand the hunt group and click **Members**.
4. Click the **Delete All** button.

Moving members of a group

Member order within a Hunt Group is important. The member order determines how a call is routed through a Hunt Group.

To move a member within a hunt group:

1. Choose **Resources**, **Telephony**, **Hunt Groups**.
2. Click a hunt group (Hunt group 1-30).
3. Expand the hunt group and click **Members**.
4. Click a member from the member list (for example Member 003).
5. On the **Configuration** menu, click **Move**.
6. Type the new member number (001, 002, etc.) in the Member box.

7. Click the **OK** button.

   The list is automatically reordered.

Assigning or unassigning lines to a group

Configure the prime set for a Hunt Group's line to None to avoid delayed ring transfer of external Hunt Group calls to the prime set before the Hunt Group can receive the call. For more information about programming line settings, see Prime set on page 102.

A line can be assigned to only one group.

To assign a line to a hunt group:

1. Choose **Resources**, **Telephony**, **Hunt Groups**.
2. Click a hunt group (Hunt group 1-30).
3. Click **Line Assignment**.
4. Click the **Add** button.
5. Type a line number (for example 061) in the line number box.
6. Click the **Save** button.

To unassign a line:

1. Choose **Resources**, **Telephony**, **Hunt Groups**.
2. Click a hunt group (Hunt group 1-30).
3. Click **Line Assignment**.
4. Click the line number (for example, Line 061) to be deleted.
5. Click the **Delete** button.

To unassign all line in a hunt group:

1. Choose **Resources**, **Telephony**, **Hunt Groups**.
2. Click a hunt group (Hunt group 1-30).
3. Click **Line Assignment**.
4. Click the **Delete All** button.

Setting the distribution mode

There are three modes of call distribution:

- Broadcast—rings each set in the group simultaneously. Calls are handled one at a time; other calls are queued. As soon as a call is picked up, the call next in the queue is presented to the Hunt Group without having to wait for queue time-out.
- In Broadcast mode, a single incoming call rings simultaneously at all the sets in a group. This way, all receptionists in the group can share the load of answering large volumes of calls. All sets automatically display the calling line identification (CLID), if available. A familiar example is a fund-raising campaign where a group of operators are waiting to take each call as it comes in.
- Linear—starts the call at the first set in the Hunt Group and distribution is complete when the first free set has been found. Simultaneous calls can be presented. Distribution is order based.
- In Linear mode, you can program your top salesperson to be the first member of the group to receive incoming calls.
- Rotary—the call starts at the set after the one which answered the last call. Distribution is complete when the next free set has been found. Simultaneous calls can be presented. Distribution is order based.
- In Rotary mode, you can ensure that all your helpline people are receiving calls on an equal basis, rather than one person receiving the majority of calls. The call rings at one set at a time in a round robin fashion.

If a Hunt Group has available members but nobody answers the call, the call is routed through the Hunt Group list until either someone answers the call or the queue time-out occurs. In the latter case, the call is routed to the overflow position. Once a call goes to the overflow position it is no longer a Hunt Group call.

To set the call distribution mode:

1. Choose **Resources**, **Telephony**, **Hunt Groups**.
2. Click a hunt group (Hunt group 1-30).
3. Click a Mode value: **Linear**, **Rotary**, **Broadcast** and press Enter.

Setting the hunt delay

This setting allows you to program the number of rings the system permits at a Hunt Group set before moving on to the next set in the Hunt Group. This attribute appears only if the distribution mode is set to Linear or Rotary. For more information, see Setting the distribution mode on page 163.

1. Choose **Resources**, **Telephony**, **Hunt Groups**.
2. Click a hunt group (Hunt group 1-30).

3. Click a Hunt Delay value: **1** to **10** and press Enter.

Programming busy line setting

A Hunt Group is considered busy if one of two scenarios exists:

- all of its members are being presented an incoming Hunt Group call
- all of its members are active on a Hunt Group call

There are three routing options if all members are busy:

- BusyTone—the caller gets a busy tone (PRI lines only)
- Overflow—the call is routed to an overflow position. If the overflow DN is the hunt group DN for that same hunt group, the overflow option will not appear.
- Queue—the call stays in the system for a period of time. Within this period of time, the call is presented to a member if one becomes available. When the time-out occurs, the call is presented to an overflow position.

1. Choose **Resources**, **Telephony**, **Hunt Groups**.
2. Click a hunt group (Hunt group 1-30).
3. Click an If busy value: **Busy Tone**, **Overflow**, or **Queue** and press Enter.

Programming the queue time-out

This setting allows you to program the number of seconds a call remains in the Hunt Group queue before it is routed to the overflow position.

1. Choose **Resources**, **Telephony**, **Hunt Groups**.
2. Click a hunt group (Hunt group 1-30).
3. Click a Queue timeout value: **15**, **30**, **45**, **60**, **120**, or **180** and press Enter.

Programming the overflow set

This setting allows you to program the overflow set to which the Hunt Group calls are to be routed. Unless the overflow position is a Hunt Group set, the call ceases to be a Hunt Group call. If the overflow set is a Hunt Group set, the call is treated as a new call and goes to the bottom of the queue.

The overflow set can be a set DN number associated with a voice mailbox.

1. Choose **Resources**, **Telephony**, **Hunt Groups**.

2. Click a hunt group (Hunt group 1-30).

3. Type the DN number in the Overflow box and press Enter.

Setting the name

This setting allows you to program the Hunt Group name, such as SERVICE or SALES. The name can be up to seven characters in length.

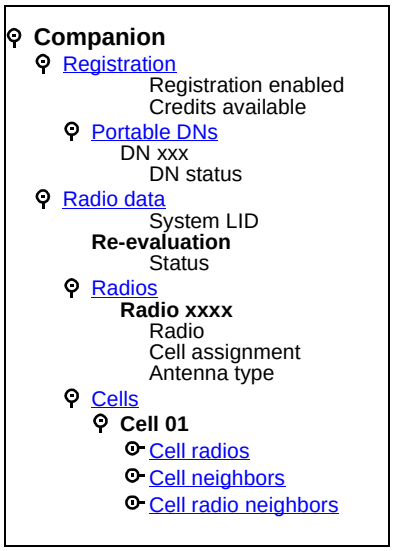
1. Choose **Resources**, **Telephony**, **Hunt Groups**.

2. Click a hunt group (Hunt group 1-30).

3. Type a new name and press Enter.

Companion

The Companion heading allows you to assign portable telephones to the system, check Base Station parameters, and enable and disable registration through programming. The following illustration shows a detailed view of the Companion programming map.



Note: Enterprise Edge Companion Wireless requires a software keycode for activation.

Registration

Software Keys are required to activate wireless capabilities
To take advantage of the wireless capabilities available to your Enterprise Edge system, you must first enable a certain number of portable credits using Software Keys.

You must enable registration for the entire Enterprise Edge system to allow registration of individual portables.

To enable user registration:

1. Select **Telephony**, **Companion.**

2. Click **Registration**.

3. Select a Registration enabled option: Y (Yes) or N (No).

Registration should normally be disabled.
For security reasons, and to prevent unauthorized users from being registered to your system, disable Registration when you have finished registering the portables.

Changing the Registration password

To ensure unauthorized portables are not registered to your system, a separate level of password access is provided. You can, and should, set your own password to prevent unauthorized handsets from registering on your system. You can change the Registration password under the Passwords heading in programming.

Change password to avoid incorrect registration.
To ensure accurate registration, change the Registration password before registering any portables. If there is another wireless system in radio range, and both systems have the same Registration password and registration enabled, you may accidentally register on the other system instead of on your own.

The default Registration password is 7 2 3 4 6 (**RADIO**).

To program a new registration password:

1. Select **Telephony**, **Passwords**.
2. Click **Registration**.
3. Enter a new password.

Tip
You can choose any combination of one to six digits. It is easier to remember the password if the digits spell a word. Provide this password only to selected personnel to prevent unauthorized access to programming. The implications of such access may include the rearrangement of line assignments, which could affect the operation of Enterprise Edge.

Portable DNs

Once registration is enabled for your Enterprise Edge system, a series of extension numbers (469 to 500) automatically becomes available for registration. Check that an extension number is available before registering a portable telephone to it.

If the extension number shows a status of Available, it is ready for registering a Companion portable telephone.

If the extension number shows a status of Registered, a Companion portable telephone is already registered to that extension number. In this case, you can either pick a different extension number, or deregister the current portable telephone. You must perform deregistration both at the portable and from the Unified Manager.

To view registered and available DNs:

1. Select **Telephony**, **Companion**, **Registration**, **Portable DNs**.

2. Click a portable DN (for example, DN 471).

Deregistering a portable

Deregister an extension number from the Unified Manager when:

- you must replace the portable due to loss or breakage
- you want to assign the handset to someone with a different telephone number than the previous user

To deregister a portable:

1. Select **Telephony**, **Companion**, **Registration**, **Portable DNs** to deregister a DN.

2. Click a portable DN (for example, DN 471).

3. Click the Configuration menu and select **Deregister**.

Tip
This procedure does not clear the registration data in the portable. You must also deregister from the portable telephone ("on-the-air" deregistration).

Radio data

Re-evaluation

Re-evaluation automatically assigns the proper cell configuration to each radio in a Base Station. When adding or removing Base Stations, Re-evaluation must be applied to the system.

Re-evaluation Status

If the Re-evaluation status reads **Required**, you can carry out the re-evaluation.

To view the Re-evaluation status:

1. Select **Telephony**, **Companion**, **Radio data**.

2. Click **Re-evaluation**.

3. Click the Configuration menu and select **Re-eval now** or **Schedule**.

Radios

Radio programming settings apply to Base Stations.

Cell assignment

A cell is the area covered by one or more radios in close proximity. As you move around your office while on a call with your portable, the call is handed off from one cell to another. A call on a portable can be handed off from one cell to another only if those cells are programmed as neighbors. The Enterprise Edge system automatically assigns cell neighbors and re-evaluates the cell-to-cell configuration when Base Stations are added or removed.

The cell assignment setting allows you to see if a Base Station radio is assigned to a cell in the Companion system.

To view the cell assignment:

1. Select **Telephony**, **Companion**, **Radio Data**, **Radios**.

2. Click **Radio nnnn**.

   where nnnn is the four-digit radio number.

Cells

Cell programming allows you to examine the cell radio, cell neighbor, and cell radio neighbor configurations. Select **Telephony**, **Companion**, **Radio Data**, **Cells** and select a cell number (01 to 32).

Cell radios

This subheading allows you to view the 5-digit number of any radios assigned to this cell. For example, if radio 07012 is in the cell, 07012 assigned is displayed. Select **Telephony**, **Companion**, **Radio Data**, **Cells**, **Cell radios** and enter the 5-digit radio number to view the setting: **Assigned** or **Unassigned**.

Cell neighbors

This subheading allows you to view the 2-digit number of any cells that border a particular cell in a system. Select **Telephony**, **Companion**, **Radio Data**, **Cells**, **Cell neighbors** and enter the cell number to see the settings: **Assigned** or **Unassigned**.

For example cell 01, Neighbour:03 and Neighbour:04 are displayed. This means that cells 03 and 04 have been assigned as cell neighbors.

Cell radio neighbors

This subheading allows you to view the 2-digit number of any cells that border a particular cell in a system (the cell neighbors) plus any cells that border the cell neighbors. Select **Telephony**, **Companion**, **Radio Data**, **Cells**, **Cell radio neighbors** and enter the cell number to see the settings: **Assigned** or **Unassigned**.

For example cell 01, Radio neighbour:03, Radio neighbour:04 are displayed, and Radio neighbour:11. Cell 11 does not appear as a cell neighbor (see the example under Cell neighbor), therefore it must be a neighbor of cell 03 or 04.

Register individual portables

You must do two things to register each portable with the Enterprise Edge system:

- Register the portables by entering the Registration password on each one.
- Verify that the portable operates properly.

When you distribute the portables, tell the users that the portables are registered and give them the corresponding extension numbers.

Tip

You can register a portable to more than one system. You cannot register a portable to more than one extension number per system. You cannot register more than one portable to one extension number.

If a portable telephone is to be used in more than one Enterprise Edge system, its owner must know which registration slot number was used to register the portable telephone with each system. (It is preferable that each user have the system they use most often registered in slot 1.)

If a portable telephone is lost or broken, deregister it from the system before replacing it with another portable telephone.

System programming

Once the registration process is complete, portable telephone programming is much the same as it is for Enterprise Edge desk telephones. Some of the programming settings do not affect the operation of the portable.

The table below shows the recommended settings for Enterprise Edge.

Programming level	Programming option	Setting	Notes
Terminals&Sets / Capabilities	Forward no answer	Fwd to: <DN> Fwd delay: <no. of rings>	
	Forward on busy	Y	
	Do Not Disturb on Busy	N	
	Handsfree	N	
	Handsfree answerback	None	
	Pickup group	<group number>	A portable can be part of a pickup group and answers calls ringing at telephones in the same group when the user enters *76.
	Paging	Y	
	Page zone	1	
	Direct-Dial	Set 1	A portable cannot be a Direct-Dial telephone. It can use the Direct-Dial digit.
	Hotline	None	
	Priority call	Y	Requires special configuration of hardware and programming
Terminals & Sets / Restrictions / Set restrictions	Set lock	Y	Does not apply to portables.
	Allow last no	Y	Does not apply to portables.
	Allow saved no	Y	Does not apply to portables.
	Allow link	Y or N	This can be set to N for portables.

Directed Call Pickup

You must turn on the Directed Call pickup feature for the system before a user can use the feature. For more information, see Capabilities on page 86.

Group Pickup

Group Pickup allows the portable user to answer a call ringing on another set in the same pickup group. Enterprise Edge programming allows you to place all telephones, including portable telephones, into pickup groups.

See Capabilities on page 86 for more information about Group pickup.

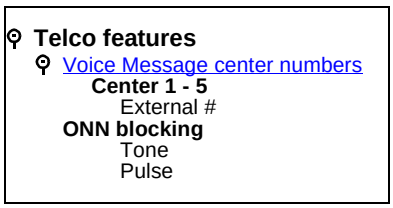
Wireless Call Forward No Answer

This stops the Companion portable from ringing when the call has been forwarded to its new destination. The portable user can still answer the call, but it does not ring.

The settings for Call Forward No Answer are found under **Terminals & Sets/ Capabilities** in the Unified Manager.

Telco features

The Telco features heading allows you define settings for voice message center numbers and outgoing name and number blocking. The following illustration shows a detailed view of the Telco features programming map.



Voice Message center numbers

If you subscribe to a voice message service outside your office, you can access it through your Enterprise Edge system. This setting specifies the external telephone numbers that are dialed by the Message feature to retrieve voice messages. Enter the external number for Center 1 through Center 5.

The default for each voice message center number is **No number**.

Tips

A telephone does not show that external voice messages are waiting unless External Voice Message set is enabled in programming. The setting is in CLASS assignment under **Terminals & Sets**.

You can program up to five voice message center numbers, but most systems require only one.

Outgoing Name and Number Blocking

Outgoing Name and Number blocking blocks the outgoing name and number on a per call basis. When this feature is used, the call is flagged to the CO so that the name and number will not be presented to the person being called. See Outgoing Name and Number Blocking on page 151 for more information.

Enter the telephone number for ONN blocking in the **Tone** or **Pulse** fields.

Software keys

The Software keys heading allows you to enter software keys to access software packages. A software key is required to order certain features or functionality groups for Enterprise Edge. The standard configuration of the system does not require a software keycode.

System Identification Number

The unique System Identification Number or System ID can be obtained by looking in the Unified Manager under **Software keys, System ID**.

Entering the software keys

1. Keys are entered in the Unified Manager by accessing **Software keys** and clicking the **Add** button**.**

2. Enter the 8 digit number for **Key 1**, **Key 2**, and **Key 3**.

3. Click **OK**. You will receive a prompt: **Entry successful**.

   Note: If the entry is unsuccessful, the prompt reads **Invalid password**. If this happens, reenter the codes or call the distributor for assistance.

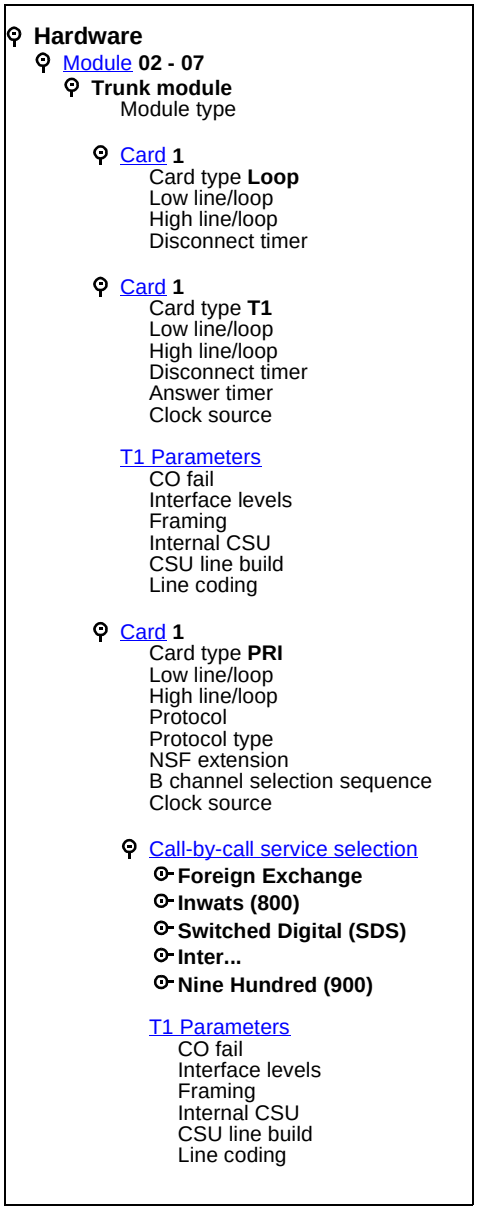
The following table indicates the various Enterprise Edge packages or products that require a keycode.

Package / Product	Features & functionality
Enterprise Edge Voice Messaging	Adds voice messaging mailboxes
Enterprise Edge Attendant Console	Attendants, server and reports functionality
Enterprise Edge Networking	Adds Voice Profile for Internet Messaging (VPIM) and Audio Messaging Interchange Specification
Enterprise Edge Call Center	Automatic Call Distribution system
Enterprise Edge Call Center Reporting	Reporting software
Enterprise Edge Router	Enables IP-based routing functionality
Enterprise Edge PRI	PRI trunks
Enterprise Edge TSP Server	TSP server, seats

Package / Product	Features & functionality
Enterprise Edge Companion Wireless	Enables wireless telephone sets to be connected to Enterprise Edge
Enterprise Edge Companion UTAM Activation (Etiquette only)	
Enterprise Edge Unified Messaging	Centralized call management
Enterprise Edge VoIP Gateway	IP telephony & VoIP ports

Hardware

The Hardware heading allows you to view and change settings for trunk modules installed in Enterprise Edge. The following illustration shows a detailed view of the Hardware programming map.



Module

Module 01 is reserved for the MSC card. As there is no hardware programming required for the MSC card, it is not displayed at this heading. You can view and perform maintenance operations on Module 01 from the Maintenance heading. For more information, see Maintenance on page 233.

Note: Because the voice over IP (VoIP) functionality resides on the MSC card, it is not necessary to program any hardware settings. The **Trunk mode** is automatically set to VoIP for lines 001 to 014. For more information, refer to the section Lines on page 95 in this chapter.

To configure a module:

1. Choose **Resources**, **Telephony**, **Hardware**, **Module**.

2. Click a Module type: **Station module**, **Analog station module**, **Trunk module** and press Enter.

   The Module type displayed depends on the hardware unit that is installed and is defined in the table below.

Module Type	Hardware unit
Station module	Digital Station Media Bay Module (EE-DSM 16 or EE-DSM32)
Analog station module	Analog Station Media Bay Module (EE-ASM 8)
Trunk module	Digital Trunk Media Bay Module (EE-DTM) CLID Trunk Media Bay Module (EE-CTM)

Card

The Card heading allows you to configure settings for the card. Options displayed depend on the type of hardware module installed in your system and the card type you select.

To program a card:

1. Choose **Resources**, **Telephony**, **Hardware**, **Module**, **Trunk Module**, and **Card 1** to access the card configuration settings.

2. Click a Card type: **Loop**, **PRI**, or **T1** and press Enter.

   Note: Provisioning PRI lines is done from the Maintenance heading. For more information, see Maintenance on page 233.

3. Configure the card settings according to the table:

Attribute	Description
Low/line loop	Automatically assigned based on the card type and the module number. For more information, see page 178. Values: View only
High line loop	Automatically assigned based on the card type and the module number. For more information, see page 178. Values: View only
Disconnect timer [1]	Allows you to specify the duration of an Open Switch Interval (OSI). For more information, see page 178. Values: 60, 100, 260, 460, or 600 milliseconds (Default: 460)
Answer timer[2]	Allows you to set the minimum duration of an answer signal before a call is considered to be answered. Values: 1, 2, 3, 4, or 5 seconds (Default: 2)
Protocol [3]	Allows you to define a trunk protocol. For more information, see page 178. Values: NI-2, DMS100, DMS250, AT&T4ESS, SL-1
Protocol type [3]	Allows you to define a protocol type. This settings applies to the SL-1 private networking protocol only. For more information, see page 178. Values: User (Slave), Network (Master) (Default: User (Slave))
NSF Extension [3]	Allows you to define the Network Specific Facilities (NSF) information element. If the prompt **Clear Routes** is displayed, click **Yes** to confirm your selection. For more information, see page 179. Values: None, WATS, ALL
B-channel selection sequence [3]	Allows you to define how B-channels are selected. For more information, see page 179. Values: Ascending Sequential, Descending Sequential
Clock Source [4]	Allows you to designate which EE-DTM acts as a primary or secondary clock source. For more information, see page 179. Values: Primary, Secondary
Notes: 1 Applies to Loop and T1 card types only. 2 Applies to T1 card types only. 3 Applies to PRI card types only. 4 Applies to PRI and T1 card types only.	

Note: There must be an EE-DTM installed if you want to program PRI or T1 trunk lines. The EE-DTM is automatically disabled and re-enabled when you change the card type. There is no need to manually enable and disable it under Maintenance.

Low line/loop High line/loop

Low line/loop and High line/loop settings are automatically assigned according to the settings in the following table. Note that Module 6 and 7 are reserved for the Companion mobility option if Companion is included in the system.

Card Type	Module 02	Module 03	Module 04	Module 05	Module 06	Module 07
T1 (Card 1)	211-234	181-204	151-174	121-144	91-114	61-84
PRI (Card 1)	211-233	181-203	151-173	121-143	91-113	61-83
Loop (Card 1)	211-214	181-184	151-154	121-124	91-94	61-64
Loop (Card 2)	219-222	189-192	159-162	129-132	99-102	69-72
Loop (Card 3)	227-230	197-200	167-170	137-140	107-110	77-80
Loop (Card 4)	235-238	205-208	175-178	145-148	115-118	85-88

Disconnect timer

Disconnect timer allows you to specify the duration of an Open Switch Interval (OSI) before a call on a supervised external line is considered disconnected. This setting must match the setting for the line at the central office (CO).

You must enable disconnect supervision by changing the **Trunk mode** attribute. From the Telephony heading, choose Lines and Line/trunk data. See Trunk/Line data on page 96 for more information.

Protocol

Enterprise Edge supports a number of different trunk protocols used by different service providers and markets. Supported protocols are listed in the table below.

Protocol	Type
NI-2, DMS100, DMS250, AT&T4ESS	Public
SL-1 (premium feature)	Private

Protocol type

When you select SL-1 protocol, an additional setting, Protocol type, appears. Because SL-1 protocol is a private networking protocol, you have the option of designating an Enterprise Edge node as a Network (Master). The default setting is User (Slave). In public network configurations, the CO is generally considered the Network side or Master.

NSF Extension

If you select the NI-2 protocol and you are using Call-by-Call services, you must specify how Enterprise Edge should handle the NSF (Network Specific Facilities)

The table below summarizes the NSF Extension settings recommended for each switch type.

Central Office	NSF Extension Setting
DMS100,	None
Siemens ESWD, Lucent 5ESS	WATS
GTD5, DMS10	ALL
The Network Specific Facilities (NSF) information element is used to request a particular service from the network. When you select **NONE**, the NSF extension bit is not set for any service. When you select **WATS**, the NSF extension bit is set for unbanded OUTWATS calls. When you select **ALL**, the NSF extension is always set for all CbC services.	

B-channel selection sequence

B-channel selection sequence allows you to select either **Ascending Sequential** or **Descending Sequential** depending on your service provider. You should choose the opposite setting of your service provider.

Note: If all lines for two EE-DTMs (configured as PRI) are in the same PRI pool, then both cards must be set to use the descending B-channel selection sequence. As a result, the service provider must use ascending sequential sequence.

Clock Source

Clock Source lets you designate which of the systems' Digital Trunk Modules (EE-DTMs) obtains the timing reference from the network to be used for synchronization.

Systems with digital interfaces need to synchronize to the network in order to function. Synchronization is done in a hierarchical way, where each device (switch) obtains the network clock from the device above it in the synchronization hierarchy and passes the network clock to the device below it in the synchronization hierarchy. The synchronization levels are referred to as strata.

Enterprise Edge systems are stratum 4E equipment and are usually used as termination points in a network.

For each EE-DTM, choose one of the following settings: **Primary**, **Secondary**, or **Master**.

Primary reference

The EE-DTM obtains the timing reference from the network and the system synchronizes to it. This is the default value for the first EE-DTM in Enterprise Edge. If the system is configured with an EE-DTM (configured as PRI), the setting should be set to Primary.

Secondary reference

The EE-DTM acts as a standby reference. If there are excessive errors on the primary T1 reference link, or the EE-DTM designated as primary reference fails, the second EE-DTM will obtain the timing reference from the network to be used for system synchronization. This is the default value for the second EE-DTM in Enterprise Edge.

Master

The EE-DTM does not obtain timing from the network, but transmits the systems timing to equipment connected to it.

Changing clock source may disconnect calls.
Changing the clock source for your system may cause your system to restart itself, resulting in dropped calls. Choose a suitable time to change the clock source and use the Page feature to inform people of possible service disruptions.

Tips
In most T1 network configurations, you need one EE-DTM configured as PRI to act as a primary reference. The only application where you might not have a PRI EE-DTM designated as a primary reference is in a network where your Enterprise Edge system is connected back-to-back with another switch using a T1 link. If the other switch is loop-timed to your Enterprise Edge system, your EE-DTM configured as PRI can be designated as a timing master.

If your Enterprise Edge system has two EE-DTMs, you cannot assign both EE-DTMs as primary reference or both EE-DTMs as secondary reference.

You can only have one primary reference and one secondary reference per system.

Call-by-call service selection

By default, incoming calls are routed based on the Called Party Number. The last ‘N’ digits of the called party number are used as Received Digits to find a target line (where ‘N’ is the Received Number Length)

For example, the incoming calling party number is 800-555-1234. The received digit number length is 4, and the result is 1234. These last four digits are used to route the call.

Depending on the protocol and the service, alternate routing maps may be defined.

1. To change the incoming call routing for a service, select a different service under **Protocol:, Call by Call Routing, FX:**.

   The first applicable service for the given protocol is displayed. In this example the service is **FX**.

2. Change the mapping that is applied to incoming calls of this service type to obtain the received digits. In all cases, the received digits are used to find a target line or to activate Remote Access.

   None: No mapping is applied. The last 'N' digits of the Called Party Number are used as received digits. Note that if there is no called party number (may occur with some FX calls) the call will ring at the incoming trunk's Prime set.

   All: Allows you to define the received digits used for all calls with this service type, regardless of the called party number or service identifier (SID). For this option, all calls with this service type on this PRI will ring the same target line.

   Map table: Allows you to associate different received digits with different calls of this service type depending on the call party number and/or the service identifier. Incoming calls that do not match any entry defined in the map table will ring at the prime set. Depending on the service type and the protocol, you may be able to map the called party number (By number) and the service identifier (SID). The following table shows the different options.

	Service				
Protocol	**FX**	**800**	**I-800**	**SDS**	**900**
NI-2	SID	By number	n/a	n/a	n/a
DMS-100	SID	SID or By number	n/a	n/a	n/a
DMS-250	SID	SID or By number	n/a	n/a	SID or By number
4ESS	n/a	By number	By number	By number	By number

Note: This setting is available for T1 trunks configured as T1 E&M. See Trunk/ Line data on page 96 for more information about configuring Trunk types.

T1 Parameters

The T1 Parameters heading appears for card types that have been configured as T1 or PRI. It allows you define a number of settings that are dependent on your T1 service provider settings.

To program T1 Parameters:

1. Choose **Resources**, **Telephony**, **Hardware**, **Module**, **Trunk Module**, and **T1 Parameters**.

2. Configure the T1 parameters according to the table:

Attribute	Description
CO fail	Allows you to select the carrier failure standard used by your T1 or PRI service provider. Consult your T1 or PRI service provider for the proper setting. Values: TIA-547A or TR62411 (Default: TIA-547A)
Interface levels	Allows you to define a loss plan setting. For more information, see page 182. Values: ISDN or PSTN (Default: ISDN)
Framing	Allows you to select the framing format used by your T1 or PRI service provider: Extended Superframe (ESF) or Superframe (SF). Contact your T1 or PRI service provider for the proper setting. (SF or Superframe is sometimes known as D4.) Values: ESF or SF (Default: ESF)
Internal CSU	Allows you to turn the internal T1 channel service unit on or off. For more information, see page 183. Values: On or Off (Default: On)
CSU line build	Allows you to set the gain level of the transmitted signal. This setting only appears when the Internal CSU is set to On. Values: 0, 7.5, or 15 dB (Default: 0)
DSX1 build	Allows you to set the distance between Enterprise Edge and an external channel service unit. This setting only appears when the Internal CSU is set to Off. Contact your service provider for the proper settings. Values: 000-100, 100-200, 200-300, 300-400, 400-500, 500-600, or 600-700 feet (Default: 000-100)
Line coding	Allows you to define the encoding signals on a T1 line. Select the standard used by your T1 service provider. Contact your T1 service provider for the proper setting. Values: B8ZS or AMI (Default: B8ZS)

Interface levels

Interface levels defaults to the ISDN loss plan setting.

Find out if your Enterprise Edge system is connected to a central office (CO) with digital network loss treatment (ISDN I/F levels) or analog network loss treatment (PSTN I/F levels) by checking with your telecommunications service provider.

The ISDN setting requires digital access lines (DAL) that have digital network loss treatment. On a DAL network, it is the PBX, rather than the CO, that administers the dB loss. DALs may have ISDN signaling or digital (such as T1 and so on) signaling. The loss plan follows the Draft TIA-464-C loss plan, which uses a send loudness rating (SLR) of 8 dB. To have DAL network loss treatment on a line with digital signaling, you must contact your service provider.

The PSTN setting requires analog access lines (AAL) that have analog network loss treatment and digital signaling. On an AAL(D) network, the CO administers the dB loss.

The loss plan follows the Draft TIA-464-C loss plan. The ISDN loss plan uses a send loudness rating (SLR) of 8 dB and a receive loudness rating (RLR) of 2 dB. The PSTN loss plan uses an SLR of 11 dB and an RLR of -3 dB. Choosing the wrong setting may affect voice quality, either too loud or too soft.

Internal CSU

Internal CSU allows you to turn the internal T1 channel service unit on or off. The channel service unit gathers performance statistics for your T1 lines or PRI with public interface. Contact your service provider for the proper settings.

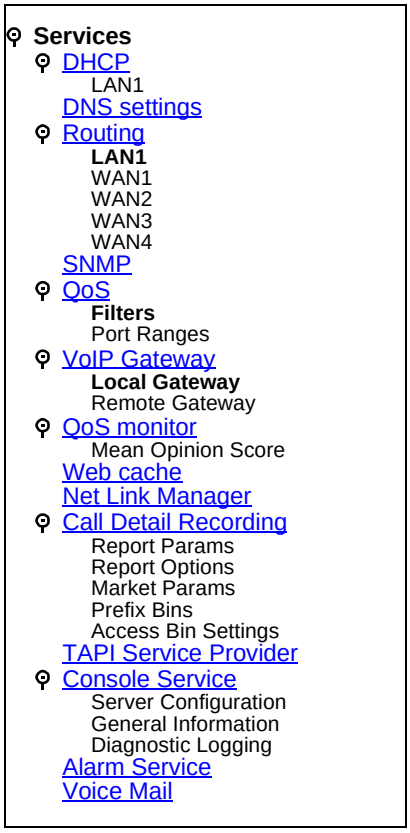
Note: You must disable the EE-DTM using Module/port status in Maintenance before you can change this setting. See Module/port status on page 254 for details.

You can view the performance statistics for your T1 lines in Maintenance under the CSU stats heading.

If you set the internal CSU off, there must be an external CSU connected to your T1 lines.

Configuring Enterprise Edge Services 7

The following shows the Services programming map:



Configuring Services attributes includes:

- DHCP on page 186
- DNS settings on page 192
- Routing on page 192
- SNMP on page 202
- QoS on page 206
- VoIP Gateway on page 212
- QoS monitor on page 215
- Web cache on page 216
- Net Link Manager on page 217
- Call Detail Recording on page 218
- TAPI Service Provider on page 223
- Console Service on page 224

- Alarm Service on page 226
- Voice Mail on page 227

Viewing Enterprise Edge services

To access the services settings:

1. On the menu click **Group** and then click **Services** or **Comprehensive**.

2. On the navigation tree click the **Enterprise Edge** key and then click **Services**. The Enterprise Edge Services table appears, which provides the name, status, version, and description of the available services. This is the same Services table that appears when you select **Enterprise Edge, System**.

3. Click the **Services** navigation key to expand the navigation tree.

DHCP

Enterprise Edge provides DHCP (Dynamic Host Configuration Protocol) service to branch office clients. This service dynamically assigns IP addresses to branch office PCs, which frees the administrator from the need to manually assign an IP address to each PC.

To configure a DHCP server, you must create a "scope" for each LAN interface in the Enterprise Edge and then allocate a block of IP addresses for that scope.

Note: Enterprise Edge retrieves many default DHCP parameters from the LAN interface parameters. Therefore, you must configure a LAN interface before you configure the DHCP server for that interface.

You must define one DHCP scope for each LAN interface. For DHCP service, there are global parameters that affect all scopes, and there are parameters that are specific for each scope.

To configure global attributes for DHCP:

1. On the navigation tree click **Services, DHCP** to view the Global Options and Summary screens for DHCP.
   Click the DHCP navigation key to expand the navigation tree, but clicking on the key doesn't display the Global Options and Summary screens. You must click **DHCP**.

   The DHCP Global Options and Summary settings appear.

The settings in the DHCP Global Options and DHCP Summary screen are:

Setting	Definition
Domain Name	Lets users specify a domain name that is passed to the client when Enterprise Edge responds to a client's DHCP requests. This setting is automatically set to 'Domain' field in 'DNS Summary' page. This means that all the DHCP clients of an Enterprise Edge server are in the same DNS domain as the Enterprise Edge server. This is also correct since Enterprise Edge runs only a DNS cache and does not introduce another DNS zone. Change the Domain setting in the DNS Summary to make a change in this setting. Occasionally you can change the value of Domain in DHCP. If you do, first make any changes to Domain in the DNS Summary to avoid overwriting your changes.
WINS Node Type	Lets users specify a clients WINS node type. Enterprise Edge automatically sets this value to 8 (indicating H-Node) if the IP Address is changed on any of the LAN interfaces. All DHCP clients of Enterprise Edge are set to h-node type when they get their IP properties from Enterprise Edge. This setting configures the DHCP client PCs to use p-node name resolution before resorting to b-node name resolution, which is efficient when there is a WINS server configured for the network. Enterprise Edge also includes a WINS server. Other options available for this field are: 1: indicates a b-node that uses broadcast mechanism for NetBIOS name resolution 2: indicates a p-node that uses point-to-point mechanism involving a WINS Server for NetBIOS name resolution 4: indicates a m-node that first uses broadcast and then point-to-point mechanism for NetBIOS name resolution.
Description	Shows a description of the Enterprise Edge server.
Version	Shows the version number of the Enterprise Edge server.
Status	Lets users enable or disable the DHCP server. When disabled, clients need to be assigned static IP addresses.

2. In the **Domain Name** box type the appropriate domain name.
   This is set in Enterprise Edge configuration. Use caution if you change it.

3. In the **WINS Node Type** box type the appropriate WINS Node Type.
   This is set in Enterprise Edge configuration. Use caution if you change it.

4. From the **Status** list box select either enable or disable.

5. Press the **Tab** key to save the settings.

DHCP LAN settings

To configure scope attributes for DHCP:

1. Click the **DHCP** navigation key to expand the navigation tree.

2. On the Navigation tree click **LAN1**.
   Clicking the LAN1 navigation key causes the key to disappear. You must click **LAN1** to display the configurable DHCP LAN1 services. If your Enterprise Edge system has multiple LAN interfaces, you can see multiple DHCP scopes under DHCP. They are named LAN1, LAN2, etc. This section describes configuring the DHCP scope for LAN1. Follow the same instructions to configure any of the parameters under the scope for LAN2.

   The frame displays the LAN Scope Specific Options, Address Range, and Excluded Address Range screens.

3. Scroll to view settings not displayed on Unified Manager.

4. Configure the scope-specific options dialog box from Unified Manager. Configure the LAN address range and the LAN excluded address services screens through the menu.

   Note: If the IP Address or subnet mask for a LAN interface is changed, the corresponding DHCP scope is created or modified for the interface. This operation also involves setting default values for some parameters. By default, Enterprise Edge sets the IP Address of corresponding LAN interface to DNS Server, WINS Server, Default Gateway options of the scope. It also sets the lease time to 3 days and creates a range of addresses for the scope. If the IP Address of the LAN interface is in the lower half of the subnet, the address range set for the scope includes all the address above the LAN interface address. If the IP Address of the LAN interface is in the upper half of the subnet, the address range set for the scope includes all the address below the LAN interface address. By default, the scope is enabled.

The DHCP LAN1 Scope Specific Options, Address Range and Excluded Address Range attributes are:

Attribute	Description
DNS Server	Lets users specify the clients' DNS server. The value for this parameter is automatically assigned by Enterprise Edge's auto-configuration system. If the IP Address or subnet mask for the corresponding LAN interface is changed, this value gets overwritten. Use caution when changing this value.
WINS Server	Lets users specify the client's WINS server. The value for this parameter is automatically assigned by Enterprise Edge's auto-configuration system. If the IP Address or subnet mask for the corresponding LAN interface is changed, this value gets overwritten. Use caution when changing this value.

Attribute	Description
Default Gateway	Lets users specify the client's default next-hop router. The value for this parameter is automatically assigned by Enterprise Edge's auto-configuration system. If the IP Address or subnet mask for the corresponding LAN interface is changed, this value gets overwritten. Use caution when changing this value.
Lease Time	Lets users specify the time, in seconds, for an address assignment until the client's lease expires.
Scope Status	Lets users enable or disable the scope.
Address Range	Lets users specify the valid IP addresses that are assigned to DHCP clients.
Excluded Address	Lets users specify IP addresses that are not available to DHCP clients.

To modify the attributes of the Scope Specific Options screen:

1. In the **DNS Server** box type the name of the DNS server.
   This field is configured automatically. Use caution when you change it.

2. In the **WINS Server** box type the name of the WINS server.
   This field is configured automatically. Use caution when you change it.

3. In the **Default Gateway** box type the default gateway.
   This field is configured automatically. Use caution when you change it.

4. In the **Lease Time** box type the lease time.
   This field is configured automatically. Use caution when you change it.

5. From the **Scope Status** list box select the scope status.

6. Press the **TAB** key to save the settings.

To modify, add, or delete a DHCP address range or excluded address range, assign only one IP Address range for a DHCP Scope and exclude ranges of addresses in it from being assigned to clients.

To modify address ranges:

1. Click an address in the address range table.

2. On the menu click **Configuration** and then click **Modify Address Ranges**.
   The Address Range dialog box appears.

3. Type the necessary changes in any of the boxes.

4. Click the **Save** button to save the modifications and return to Unified Manager.

To add an address range:

1. On the menu click **Configuration** and then click **Add Address Range**.
   The Address Range dialog box appears.

2. In the **Range** box type the range identifier.
   The range field uniquely identifies a range value in the scope. The value for this field is used as key, and must follow certain conventions. It must always start with the prefix 'R' followed by a unique number identifying the range in the table. For example, 'R2' is a valid name.While adding, specify non-recurring values for the unique number. While adding, if you specify an existing range name, it modifies the existing range. Using non-sequential numbers results in automatic reassignment of sequential numbers. When you modify a range, you can't change the range name. The range name does not have any significance other than identifying an entry.

3. In the **Start Address** box type the start address.

4. In the **End Address** box type the end address.
   Scroll to see any fields that are not displayed.
   Make sure the start address and end address are in the same subnet.

5. Click the **Save** button to save the address range and return to Unified Manager.

To delete an address range:

1. Click an address in the **Address Range** table.

2. On the menu click **Configuration** and then click **Delete Address Ranges**.
   A message appears asking you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

   Note: Deleting or modifying an IP Address range removes any excluded addresses that are completely contained in the original address range value.

To modify excluded address ranges:

1. Click an excluded address in the **Excluded Address Range** table.

2. On the menu click **Configuration** and then click **Modify Excluded Address Ranges**.
   The Excluded Address Range dialog box appears.

3. In any box that requires modification type the necessary changes.

4. Click the **Save** button to save the modifications and return to Unified Manager.

To add excluded address ranges:

1. On the menu click **Configuration** and then click **Add Excluded Address Range**.
   The Excluded Address Range dialog box appears.

2. In the **Range** box type the range identifier.

   Note: The range field uniquely identifies an excluded range value in the scope. The value for this field is used as key, and must follow certain conventions. It must always start with the prefix 'E' followed by a unique number identifying the range in the table. For example, 'E2' is a valid name. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing excluded range name, it modifies the existing range. Using non-sequential numbers results in automatic reassignment of sequential numbers. When you modify an excluded range, you can't change the range name. The excluded range name does not have any significance, other than uniquely identifying an entry.

3. In the **Start Address** box type the start address.

4. In on the **End Address** box type the end address.
   Scroll to see any fields that are not displayed.

   Note: Make sure the start address and end address are in the same subnet, and an excluded address range is completely contained in an IP address range specified for the subnet.

5. Click the **Save** button to save the excluded address range and return to Unified Manager.

To delete an excluded address range:

1. Click an excluded address in the **Excluded Address Range** table.

2. On the menu click **Configuration** and then click **Delete Excluded Address Ranges**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

4. Click the **DHCP** navigation key to close the navigation tree.

DNS settings

To configure DNS services settings, select **Services, DNS** from the navigation tree. This brings you to the DNS Summary screen.

The DNS Summary attributes are:

Attribute	Description
Description	Lets users view the description of the server in cache mode.
Version	Lets users view the version of the software interface.
Status	Lets users enable or disable the DNS cache proxy in Enterprise Edge.
Domain	Lets users specify the domain name that Enterprise Edge and its DHCP clients uses. When modified, contents of this setting are automatically copied to Domain Name global options (O15) under DHCP.
Primary Server	Lets users specify the primary server IP address in a valid dot format. More than one address can be specified separated by a space; DNS cache uses them in the specified order to resolve names.
Forward Timeout	Lets users specify the time-out, in seconds, used in resolving queries using the DNS servers that are specified in DNS server.

To modify the configuration of the DNS summary:

1. From the **Status** list box select the status.
2. In the **Domain** box type the domain.
3. In the **Primary Server** box type the primary server.
4. In the **Forward Timeout** box type the forward timeout.
5. Press the **Tab** key to save the settings.

Routing

To configure Routing services settings, select **Services, Routing** from the navigation tree. This brings you to the Routing Summary and Global Settings screens.

The Routing Summary and Global Settings attributes are:

Attribute	Description
Description	Shows a description of the router.
Version	Shows the version of the router.
Status	Lets users enable or disable the router.

Attribute	Description
Packet Filtering	Lets users enable or disable packet filtering. When the system comes up the first time, this value is N/A, indicating that the Management system cannot retrieve pertinent information. Set it to Disabled or Enabled and valid values are displayed. Disabling packet filtering here disables it on all interfaces. The router performs better when packet capturing is disabled.
RIP Log Level	Lets users specify a log-level for the RIP routing protocol manager: maximum generates the maximum log warnings also, generates a log for warning conditions too errors only, generates log errors only (for use during normal operations) disabled disables logging (not recommended).
Triggered Update Interval	Lets users specify the minimum interval between sending triggered updates.

To modify the attributes of the Routing Summary and Global Settings screens:

1. From the **Status** list box enable or disable the router.
2. From the **Packet Filtering** list box enable or disable packet filtering.
3. From the **RIP Log Level** list box select the RIP log level.
4. In the **Triggered Update Interval** box type the triggered update interval.
5. Press the **TAB** key to save the settings.

LAN Routing

This section describes the instructions to configure LAN1 interfaces for routing. If there are other existing LAN or WAN interfaces, they also appear in Routing. Follow the same instructions to configure them.

1. On the navigation tree click the **Routing** navigation key to expand the menu.
2. On the navigation tree click **LAN1**.
   Clicking the LAN1 navigation key causes the key to disappear. You must click LAN1 to view the available services to configure.
   The Summary, Input Filters, Output Filters, and Static Route screens appear.

   Note: The RIP Parameters screen is not displayed unless you choose RIP as your routing protocol in the LAN1 summary screen. To display the RIP parameters, click the **Routing Protocol** list box and choose RIP. Then press the **Tab** key to update the screen. A configurable RIP screen appears.

   You configure the LAN1 (and WAN1, WAN2, etc.) Routing Summary screen from Unified Manager.

The Input Filters, Output Filters, and Static Route screens are configured through the menu.

The LAN1 Routing Services Summary and RIP Parameters attributes are:

Attribute	Description
Routing Protocol	Lets users select the Routing protocol to run over the interface. Select RIP to run RIP protocol or select NONE to disable running any routing protocol. If RIP is selected, interface-specific RIP parameters appear in the bottom of the screen. You can configure other RIP parameters on this interface
Input Filter Action	Determines what action is performed for the packets that match the filter criteria. You can either forward them to upper layer, possibly for further routing or drop them. You can select the action only if you have set any of the input or output filters. Otherwise, they show up as N/A and you can't modify them.
Output Filter Action	Determines what action is performed for the packets that match the filter criteria. You can either forward them to the next hop or drop them. You can select the action only if you have set any of the input or output filters. Otherwise, they show up as N/A and you can't modify them.
Metric	Specifies the associated metric value for the routes through this interface. Metric values of all routes learned through this interface are incremented by this value. The final value used in making routing decisions is forwarded to other routes through RIP updates.
Routing Table Update Mode	Lets users specify the routing table update mode for the interface. In On Demand mode, the router sends its table when requested by another established router. In Periodic mode, the router sends its table to other established router at regular intervals.
Route Announcement Type	Lets users specify the route-announcement type for the specified interface. The choices are: Disabled: sending RIP packets is disabled on this interface. This requires the other routers in the subnet have static routes configured to access the Enterprise Edge server. RIP 1: sends RIP v1 packets in broadcast only. RIP 1 Compatible: sends RIP v1 and RIP v2 packets in broadcast. Use this for a mixed environment of RIP v1 and RIP v2 RIP 2: sends RIP v2 packets in multicast only. Use this only if all other routers connected to the Enterprise Edge server are RIP v2 capable.
Route Accept Type	Lets users choose to accept announcements in either RIP1, RIP2, or both formats. The choices are: Disabled: accepting RIP packets is disabled. If this choice is selected, the user is prompted to create static routing entries in the Enterprise Edge server to access other networks connected through this interface. This method is preferable if you want to keep the routing table small in the Enterprise Edge server. RIP 1: accepts only RIP v1 packets RIP 1 Compatible: accepts packets of both RIP v1 and RIP v2 RIP 2: accepts only RIP v2 packets.
Route Expiration Interval	Lets users specify, in seconds, the time interval to mark an established router that has not updated its table eligible for removal.

Attribute	Description
Route Removal Interval	Lets users specify, in seconds, the time interval between route expires and when it is removed from the routing table.
Route Announcement Interval	Lets users specify, in seconds, the time interval between route announcements.
Route Tag	Lets users create a special tag that is included in routes announced over the interface. This helps identify route packets while debugging routing problems using a network sniffer.
Poisoned Reverse	Lets users enable poison reverse. The choices are: Actual: the actual, original RIP updates are performed over this interface. All the routes learned through this interface are also included as is in the RIP updates sent over this interface. This leads to mutually deceiving route updates that require multiple routing updates that is termed 'counting to infinity' in RIP terms. Split: in the routing updates sent over this interface, router does not include the routes learned over this interface. This mode performs better than Actual, but still requires significant amount of time to converge routes. It requires all routes corresponding to an unreachable network expire before removing them from the routing table Poison Reverse: in the routing updates sent over this interface, the router includes the routes learned over this interface, but 'poisoned metrics'. All metric values are set to RIP infinity (16) for the routes learned through this interface. This results in the fastest convergence.
Triggered Updates	Lets users enable triggered updates, or immediate route update announcements whenever a metric or other parameter changes in the route table entries. If triggered updates are enabled, the changes are gathered for the interval specified in the global parameter Triggered Update Interval and then sent over this interface. Triggered updates results in more frequent, smaller RIP updates.
Announce Default Route	Lets users enable or disable announcing default routes in incoming route announcements. Use caution when enabling this feature as improper configuration causes a loss of network connectivity. Default routes are always set statically on the router.
Accept Default Route	Lets users enable or disable accepting incoming default routes. Set default routes as static routes. If you are run Net Link Manager to automatically backup primary WAN link using a dial-up link, it manages the default routes and the default routes that you add are non-operational as soon as a link breaks or comes up.

To modify the configuration of the LAN1 routing summary screen:

1. From the **Routing Protocol** list box select **NONE** or **RIP**.
   If you choose RIP, press the **Tab** key to update the screen.
   A configurable RIP Parameters screen appears.

2. From the **Input Filter Action** list box select the input filter action.

3. From the **Output Filter Action** list box select the output filter action.

4. Press the **Tab** key to save the settings.
   This operation fails if filters have not been added to the interface.

To modify the configuration of the RIP Parameters:

1. Scroll to locate the RIP Parameters screen.

2. In the **Metric** box type the cost integer value.

3. From the **Routing Table Update Mode** list box select the mode.

4. From the **Route Announcement Type** list box select the routing announcement.

5. From the **Route Accept Type** list box select the route accept type.

6. In the **Route Expiration Interval** box type the expiration interval value in seconds.

7. In the **Route Removal Interval** box type the removal interval value in seconds.

8. In the **Route Announcement Interval** box type the announcement interval value in seconds.

9. In the **Route Tag** box type the route tag.

10. From the **Poisoned Reverse** list box select the appropriate mode.

11. From the **Triggered Updates** list box enable or disable triggered updates.

12. From the **Announce Default Route** list box enable or disable announcing default routes.

13. From the **Accept Default Route** list box enable or disable accepting default routes.

14. Press the **Tab** key to save the settings.

The LAN1 Filter and Static Route attributes are:

Attribute	Description
Input filter	Specifies the filter name and identifies an individual input filter on the specified interface. Its value must follow certain conventions. It must have the prefix IF followed by a unique number that identifies the input filter on the interface. For example, IF2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing filter name, it modifies the existing filter. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a filter, you can't change the name. The filter name does not have any significance other than to identify an entry.
Output filter	Specifies the filter name and uniquely identifies an individual output filter on the specified interface. Its value must follow certain conventions. It must have the prefix OF followed by a unique number that identifies the input filter on the interface. For example, OF2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing filter name, it modifies the existing filter. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a filter, you can't change the name. The filter name does not have any significance other than to identify an entry.
Source address	Lets users specify the source IP address in a valid dot format. If you don't want to match the source address field in your filter, leave this setting and the source mask empty.
Source mask	Lets users specify the source mask for the IP address in a valid dot format. If you specify a source address, you must specify the source mask. If you don’t specify the source address, you must not specify the source mask. The source address and source mask must match. Bitwise, the source address and the source mask must be equal to the source address.
Destination address	Lets users specify the destination IP address in a valid dot format. If you are specifying a filter, this field specifies the destination address of the IP packet that matches the filter. If you don't want to match the destination address, leave this field empty. If you are specifying a static route, this field must not be empty. It must be a valid network or host address.The destination mask must match the address specified in this setting.
Destination mask	Lets users specify the mask of the destination address in a valid dot format. If you specify a destination address, you must specify a destination mask. If you don’t specify the destination address, you must not specify the source mask. The destination address and destination mask must match; i.e. bitwise AND of destination address and destination mask should be equal to destination address.

Attribute	Description
Protocol	Lets users specify the protocol to match the filter. The choices are: TCP: look for the TCP protocol packets. You can specify source and destination service ports in other fields. If you don't specify any port numbers all packets that match this protocol and other criteria, if any, match the filter. UDP: look for UDP protocol packets. You can further specify source and destination service ports in other fields. If you don't specify any port numbers all packets that match this protocol and other criteria, if any, match the filter. ICMP: look for ICMP protocol packets. You can further specify the ICMP message types and ICMP codes in other fields. If you don't specify any ICMP types or codes all packets that match this protocol and other criteria, if any, match the filter.
Source port/ ICMP type	If the protocol chosen is UDP or TCP, this lets users specify the source port to match the filter. If the protocol chosen is ICMP, this field specifies the ICMP code value to look for in the packet to match the filter. Destination Port/ICMP Code: If the protocol chosen is UDP or TCP, this lets users specify the additional destination service port to match the filter. If the protocol chosen is ICMP, this field can contain the optional ICMP code.
Static Route	Specifies the static route name and is used as a key to uniquely identify an individual static route on the specified interface. Its value must follow certain conventions. It must have the prefix SR followed by a unique number that identifies this static route on this interface. For example, SR2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing static route name, it modifies the existing static route. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a static route, you can't change the name. The static route name does not have any significance other than to identify an entry.
Next Hop Router	Lets users specify the IP address in a valid dot format for the next hop router.
Metric Value	Lets users specify the metric value associated with the interface. The metric is added to the hop count of the routes received through the interface.

Note: If input and output filters are not defined for the LAN1 interface, modifying input filter action or output filter action in the summary causes an error message.

To modify the configuration of LAN1 input filters:

1. Select an **input filter** in the input filter table.

2. On the menu click **Configuration** and then click **Modify Input Filter**. The Input Filters dialog box appears.

3. In the **Source Address** box type the source address.

4. In the **Source Mask** box type the source mask.

5. In the **Destination Address** box type the destination address.

6. In the **Destination Mask** box type the destination mask.

7. From the **Protocol** list box select the response.

8. In the **Source Port/ICMP Type** box type the source port/ICMP type.

9. In the **Destination Port/ICMP Type** box type the destination port/ICMP type.

10. Click the **Save** button to return to Unified Manager.

To add LAN1 input filters:

1. On the menu, click **Configuration** and then click **Add Input Filter**. The Input Filter dialog box appears.

2. In the **Input Filter** box type the input filter.

3. In the **Source Address** box type the source address.

4. In the **Source Mask** box type the source mask.

5. In the **Destination Address** box type the destination address.

6. In the **Destination Mask** box type the destination mask.

7. From the **Protocol** list box select the response.

8. In the **Source Port/ICMP Type** box type the source port/ICMP type.

9. In the **Destination Port/ICMP Type** box type the destination port/ICMP type.

10. Click the **Save** button to return to Unified Manager.

To delete LAN1 input filters:

1. Click a filter in the **Filter** table.

2. On the menu, click **Configuration** and then click **Delete Input Filter**. A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

To modify the configuration of LAN1 output filters:

1. Click an output filter in the **Output Filter** table.

2. On the menu, click **Configuration** and then click **Modify Output Filter**.

3. Follow the steps for modifying input filters.

To add LAN1 output filters:

1. On the menu, click **Configuration** and then click **Add Output Filter**. The Output Filter dialog box appears.

2. In the **Output Filter** box type the output filter.

3. In the **Source Address** box type the source address.

4. In the **Source Mask** box type the source mask.

5. In the **Destination Address** box type the destination address.

6. In the **Destination Mask** box type the destination mask.

7. From the **Protocol** list box select the response.

8. In the **Source Port/ICMP type** box type the source port/ICMP type.

9. In the **Destination Port/ICMP type** box type the destination port/ICMP type.

10. Click the **Save** button to return to Unified Manager.

To delete LAN output filters:

1. Click on an output filter in the **Output Filter** table.

2. On the menu, click **Configuration** and then click **Delete Output Filter**.

3. Follow the steps for deleting input filters.

To modify the configuration of static routes:

1. Click a static route in the **Static Route** table.

2. On the menu, click **Configuration** and then click **Modify Static Route**. The Static Route dialog box appears.

3. In the **Destination Address** box type the destination address.

4. In the **Destination Mask** box type the destination mask.

5. In the **Next Hop Router** box type the next hop router.

6. In the **Metric Value** box type the metric value.

7. Click the **Save** button to return to Unified Manager.

To add LAN1 static routes:

1. On the menu, click **Configuration** and then click **Add Static Route**.
   The Static Route dialog box appears.

2. In the **Static Route** box type the static route.

3. In the **Destination Address** box type the destination address.

4. In the **Destination Mask** box type the destination mask.

5. In the **Next Hop Router** box type the next hop router.

6. In the **Metric Value** box type the appropriate metric value.

7. Click the **Save** button to return to Unified Manager.

To delete LAN static routes:

1. Click a static route in the **Static Route** table.

2. On the menu, click **Configuration** and then click **Delete Static Route**.

3. Follow the steps for deleting input filters.

WAN Routing

To configure WAN routing services:

1. Click the **Routing** navigation key to expand the navigation tree.

2. On the navigation tree, click **WAN1** or **WAN2**.
   Clicking the WAN1 or WAN2 navigation key causes the key to disappear. You must click WAN1 or WAN2 to view the configurable WAN resources.

   The Summary, RIP Parameters, Input Filters, Output Filters, and Static Route screens appear.

   Note: The RIP Parameters screen is not displayed unless RIP is chosen as your routing protocol in the WAN summary screen. To display the RIP parameters, click the **Routing Protocol** list box and select RIP. Then press the **Tab** key to update the screen. A configurable RIP screen appears.

3. Use the scroll bars to locate any fields that are not displayed.

4. Configure the WAN1 or WAN2 routing summary and RIP Parameters screens from Unified Manager.
   Configure the input filters, output filters, and static route attributes from the menu.

5. Follow the steps outlined in LAN routing settings to complete your configuration process.

6. Clicking the **Routing** navigation key to close the navigation tree.

SNMP

To configure SNMP services settings:

1. On the navigation tree click **SNMP**.
   Clicking the SNMP navigation key causes the key to disappear. You must click SNMP.

   The screen displays the SNMP Summary, Community List, Manager List, and Trap Community List screens.

2. Configure SNMP summary screen from Unified Manager.
   Configure the SNMP Community List, Manager List, and Trap Community List from the menu.

The SNMP Summary attributes are:

Attribute	Description
Description	Shows the description of the SNMP agent.
Version	Shows the version of the SNMP agent
Status	Lets users enable or disable the SNMP agent.
Authentication Failure Traps	Lets users enable or disable authentication failure traps. When enabled, the SNMP agent sends authentication failure traps if there is an authentication failure. Authentication failure happens if an SNMP manager application provides a wrong community string or performs an operation that is not permitted for a community.

To modify the SNMP Summary attributes:

1. From the **Status** list box select **enable** or **disable**.

2. From the **Authentication Failure Traps** list box select **enable** or **disable**.

3. Press the **Tab** key to save the changes.

SNMP Community List, Manager List, and Trap Community List

The SNMP community list, manager list, and trap community list attributes are:

Attribute	Description
Community List	Lets users specify the entry name used as a key to uniquely identify an individual community entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix C followed by a unique number that identifies the community name entry on the agent. For example, C2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing community entry name, it modifies the existing community entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a community entry, you can't change the name. The community entry name does not have any significance other than to identify an entry.
Community Name	Lets users specify the name of the community that the individual managers use to interact with this agent. When creating community entries, various access permissions are associated with these names. Manager stations that use different community names get different permissions on the SNMP agent. While creating trap communities, various manager IP addresses are associated with these values. All the manager stations in a trap community get traps with the community name specified in the entry.
Manager List	Lets users specify the entry name used to identify an individual manager entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix M followed by a unique number that identifies the manager entry on the agent. For example, M2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing manager entry name, it modifies the existing manager entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a manager entry, you can't change the name. The manager entry name does not have any significance, other than to uniquely identify an entry.
Manager IP address	Lets users specify the IP Address of the SNMP Manager station corresponding to this entry. If no manager entries are created, the Enterprise Edge device accepts SNMP requests from all stations. If there is a list of manager entries, Enterprise Edge server accepts SNMP requests from the IP Addresses specified in the list.
Trap List	Lets users specify the entry name used to identify an individual trap community entry on the SNMP agent. Its value must follow certain conventions. It must have the prefix T followed by a unique number that identifies the trap community entry on the agent. For example, T2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing trap community entry name, it modifies the existing trap community entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a trap community entry, you can't change the name. The trap community entry name does not have any significance, other than to uniquely identify an entry.

To modify the Community List, Manager List, and Trap Community List, use the following procedures.

To add to the community list:

1. On the menu, click **Configuration** and then click **Add Community**. The Community List dialog box appears.

2. Click the **Community List** box and type the community list.

3. Click the **Community Name** box and type the community name.

4. Scroll to view the **Access Permission** settings.

5. From the **Access Permission** the list box select the Access Permission.

6. Click the **Save** button to return to Unified Manager.

To modify a community:

1. Click a community in the **Community** table.

2. On the menu, click **Configuration** and then click **Modify Community**. The Community List dialog box appears.

3. Click any box that requires modification and type the necessary changes.

4. Click the **Save** button to return to Unified Manager.

To delete a community:

1. Click on a community in the **Community** table.

2. On the menu, click **Configuration** and then click **Delete Community**. A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

To add a manager to the Manager List:

1. On the menu, click **Configuration** and then click **Add Manager**. The Manager List dialog box appears.

2. In the **Manager List** box type the manager list.

3. In the **Manager IP Address** box type the manager IP address.

4. Click the **Save** button to return to Unified Manager.

To modify the manager list:

1. In the **Manager List** table, click a manager.

2. On the menu, click **Configuration** and then click **Modify Manager**.
   The Manager List dialog box appears.

3. Click any box that requires modification and type the necessary changes.

4. Click the **Save** button to return to Unified Manager.

To delete a manager:

1. In the **Manager** table, click the manager you want to delete.

2. On the menu, click **Configuration** and then click **Delete Manager**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

To add a trap community to the Trap Community List:

1. On the menu, click **Configuration** and then click **Add Trap Community**.
   The Trap Community List dialog box appears.

2. In the **Trap List** box type the trap list.

3. In the **Community Name** box type the community name.

4. Scroll to see the **Manager IP Address** box.

5. In the Manager IP Address box, type an IP Address for a manager station that is a member of this trap community.

6. Click the **Save** button to return to Unified Manager.

To modify a trap community:

1. In the **Trap Community** table, click the trap community you want to modify.

2. On the menu, click **Configuration** and then click **Modify Trap Community**.
   The Trap Community List dialog box appears.

3. Click any box that requires modification and type the necessary changes.

4. Click the **Save** button to return to Unified Manager.

To delete a trap community:

1. In the **Trap Community** table, click the trap community you want to delete.

2. On the menu, click **Configuration** and then click **Delete Trap Community**. A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

QoS

To configure QoS services settings:

1. On the navigation tree click **QoS**.
   Clicking the QoS navigation key expands the navigation tree but doesn't display the summary of configurable QoS services. You must click **QoS**.

   The QoS Summary screen appears. The QoS Services Summary attributes are:

Attribute	Description
Description	Shows the description of the QoS provider.
Version	Shows the driver version of the QoS provider.
Status	Lets users enable or disable the QoS module.
Premium Bandwidth	Lets users specify, in percentages, the WAN bandwidth reserved for premium traffics. Choose a value for this field based on the link speed, the codecs used by VoIP gateway, the sample rate and the number of concurrent phone calls (from internal VoIP gateway) and other H.323 sessions (like Microsoft NetMeeting traffic) you intend to carry over the WAN link. Refer to the figure WAN overview on page 49 for more information on this topic. Make sure you allocate at least the bandwidth necessary to carry as many phone calls as specified in 'Number of Phone Ports' field below. Otherwise, the QoS provider sees the inconsistent configuration and disables itself when system boots next time, resulting in broken connectivity. Any additional bandwidth that is more than what is required to carry the phone calls is available for other H.323 sessions like NetMeeting sessions from PCs connected to Enterprise Edge box or other data traffic classified as premium, through QoS Filters. This additional bandwidth reserved for premium traffic is always available for other data traffic if there is no additional H.323 traffic or other premium traffic. A network administrator can reserve more WAN bandwidth than that required to carry phone calls and then prevent PC users from using it for NetMeeting sessions by setting filters that drop H.323 traffic at LAN interfaces.
Video Class	Lets users specify the type of priority treatment for video traffic in H223 sessions. The following choices are available: Premium: Video traffic is treated as premium traffic that consumes portions of bandwidth reserved for premium traffic (Premium Bandwidth field). Best Effort: Video traffic is treated as best effort IP traffic that are prioritized among other best-effort traffic passing through the WAN link.

Attribute	Description
Premium DS Code	Lets users specify the TOS field in the IP header for premium packets. This value is used in conjunction with the frame relay driver in Enterprise Edge's WAN link, if one is being used, as well as rest of the network. If the frame relay is used on WAN link, this code should match the DS Code field in frame relay settings so that frame relay network treats this traffic as high-priority. If rest of the network is diffserv capable, all routers that carry VoIP traffic from theEnterprise Edge server must be configured to treat the traffic with this DS code as high-priority or premium traffic.
Number of Phone Ports	Lets users specify the number of phone ports. This value specifies the number of concurrent phone calls user intends to carry over the WAN interface. QoS Provider layer uses this value to determine how much of the bandwidth reserved for premium traffic is consumed by internal VoIP gateway and how much is left over for other H.323 or other classified premium traffic.
Filter Order	Lets users specify the order that filters are evaluated. If a filter name is listed in filter order, but the actual filter is missing, it is ignored. If an actual filter is omitted from the filter order list, the filter is not effective.
Filter	Lets users specify the entry name that is used as a key to uniquely identify an individual filter entry in QoS layer. Its value must follow certain conventions. It must have the prefix F followed by a unique number that identifies this filter. For example, F2 is a valid value. While adding, specify non-recurring values for the unique number. While adding, if you specify an existing filter entry name, it modifies the existing filter entry. Using non-sequential numbers results in automatic reassignment of sequential numbers. While modifying a filter entry, you can't change the name.
Source Address	Lets users specify the source IP address in a valid dot format. If you want to ignore the source address field in filter, leave this field blank. If you specify an address in this field, you should also specify a subnet mask in the Source Mask field.
Source Mask	Lets users specify the source mask of the IP address in a valid dot format. If you specify a source address, you must specify a source mask and vice versa. Make sure that the mask and address match with each other, i.e. bitwise and of mask and address is equal to the address. If you want to specify a range of addresses, use a subnet mask other than 255.255.255.255. For example, address/mask combination 10.10.10.32/ 255.255.255.252 represents addresses 10.10.10.32-10.10.10.35.
Destination Address	Lets users specify a destination IP address in a valid dot format. See the instructions for Source Address.
Destination Mask	Lets users specify a mask for the destination IP address in a valid dot format. See the instructions for Source Mask.

Attribute	Description
Source Port	Lets users specify a source port to match the filter. Specify a source port only if you choose a TCP or a UDP protocol. If you don't want to include the source port in your filter, select IGNORE for it. Otherwise, select the port for one of the well-known services from the list or type it in the list box. If you type the port, specify the service's numeric port number. You can specify a range of ports by specifying the two limits of the range by a hyphen character, for example, 156-159. You can also specify 0 for the lower limit and 65536 for upper limit.
Destination Port	Lets users specify a destination port to match the filter. It is interpreted the same way as source port.
Protocol	Lets users specify a protocol to match the filter. If you don't want to include a protocol in your filter, select IGNORE for the protocol. Otherwise, select the protocol from the list or type the numeric value of sub-protocol under IP in the box.
PortRange	Lets users reserve and list different UDP port ranges that the Enterprise Edge QoS module uses for VoIP RTP flows. Set the UDP ports to high priority so that VoIP packets are forwarded quickly.
DSCode (TOS) Criteria	Lets users specify the DS Code (TOS) value for the filter to match. Use this setting only if your network or application behind Enterprise Edge is diffserv capable or diffserv aware. Specify here the DS Code or TOS value that the application or the other edge device puts in the IP packets it sends. Otherwise, ignore this setting.
Priority	Lets users specify the priority given to packets that match the criteria specified in the filter. The priority value has significance only within the IP interface the packet is related, and is relative to other packets that go out through the interface. 0 is the highest priority and 8, the lowest priority. Use caution when you assign priority. If you assign priority 0 for regular data traffic, it is possible that the quality of voice calls that go through this interface are degraded. Use priority 0 only if your WAN does not carry any voice calls. As a guideline, always start assigning priorities from the lowest level up.
Outbound DS Code	Lets users specify the new DS Code added to the packets that match this filter. If you don't want to change the DS Code in the packets going out through the interface, don't specify any value for this setting. If a value is specified, this setting lets Enterprise Edge change the DS code on outgoing packets. This lets Enterprise Edge be used as a 'marker' device on the edge of a diffserv capable network.

2. In the **Description** box type the description.
3. In the **Version** box type the version.
4. From the **Status** list box select enable or disable.
5. In the **Premium Bandwidth** box type the appropriate premium bandwidth.
6. From the **Video Class** list box select the video class.
7. In the **Premium DS Code** box type the premium DS code.

8. In the **Number of Phone Ports** box type the number of phone ports.

9. Press the **Tab** key to save the settings.

QoS performance graphs and tables

To access QoS performance graphs and tables:

1. On the menu, click **Performance** and then click **QoS Session Graph**.
   The QoS Performance Graph appears.

Note: For information on using performance tables and graphs, refer to Graphs and tables on page 243.

2. On the menu, click **Performance** and then click **QoS Session Table**.
   The QoS Performance Table appears.

3. Access the remaining QoS graphs and QoS tables by following the steps for QoS Session Graphs and Tables.

QoS filters

To set the QoS filters:

1. Click the **QoS** navigation key to expand the navigation tree.

2. On the navigation tree, click **Filters**.
   Clicking the Filters navigation key causes the key to disappear. You must click **Filters**. The Filters Configuration and Filters screens appear.

3. In the **Filter Configuration** box type the filter configuration.

4. Press the **Tab** key to save the settings.

To modify QoS filters:

1. In the Filter table, click the filer you want to modify.

2. On the menu, click **Configuration** and then click **Modify Filter**.
   The Filters dialog box appears.

3. Make changes to any setting that you want to modify.

4. Click the **Save** button to return to Unified Manager.

To add QoS filters:

1. On the menu, click **Configuration** and then click **Add Filter**.
   The Filters dialog box appears.

2. In the **Filter** box type the appropriate filter.
   Type a name that looks like “Fxx” where “xx” is a unique integer in the filter table.

3. In the **Source Address** box type the source address if it is required or leave this box empty.

4. In the **Source Mask** box type the source mask.
   If you specify a source address, you must specify a source mask.

5. In the **Destination Address** box type the destination address if it is required or leave this box empty.

6. In the **Destination Mask** box type the destination mask or leave this box empty.

7. From the **Source Port** list box, if required, select the source port or select ignore.

8. From the **Destination Port** list box select the destination port.

9. From the **Protocol** list box if required, select the protocol or click ignore to ignore this field.

10. In the **DSCode (TOS) Criteria** box select a DS code in hex or leave this setting blank.

11. From the **Priority** list box select the priority.
    Use caution when selecting a priority. Lower values have precedence over higher values. For priority 0, Enterprise Edge gives the same precedence as voice traffic, possibly affecting the latter adversely.

12. In the **Outbound DS Code (TOS)** box type the outbound DS code.

13. Click the **Save** button to return to Unified Manager.

To delete QoS filters:

1. On the **Filter** table, click the filter you want to delete.

2. On the menu, click **Configuration** and then click **Delete Filter**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

QoS Port Ranges

To set the QoS port ranges:

1. Click the **QoS** navigation key.

2. On the navigation tree, click **PortRanges**.
   Clicking the Port Ranges navigation key causes the key to disappear. You must click **PortRanges**.

   The QoS PortRanges screen appears.

To modify port ranges:

1. In the **Port Ranges** table, click the port ranges you want to modify.

2. On the menu, click **Configuration** and then click **Modify Port Ranges**.
   The Port Ranges dialog box appears.

3. In the **Begin** box.type the beginning value for the range.
   This must be an even value.

4. In the **End** box type the appropriate end value for the range.

5. Click the **Save** button to return to Unified Manager.

To add port ranges:

1. On the menu, click **Configuration** and then click **Add Port Ranges**.
   The Port Ranges dialog box appears.

2. In the **PortRange** box type the port range.
   Type an entry that looks like “Rxx” where “xx” is a unique integer.

3. In the **Begin** box type the beginning value for the range.
   This must be an even value.

4. In the **End** box type the ending value for the range.

5. Click the **Save** button to return to Unified Manager.

   Note: If the rest of your network is not diffserv capable, you can set filters in other routers to give higher priority to VoIP traffic. In all the routers that carry VoIP traffic from the Enterprise Edge server, you must set filters that classify the traffic to and from these port ranges as high-priority.

To delete port ranges:

1. In the **Port Ranges** table, click the port ranges you want to delete.

2. On the menu, click **Configuration** and then click **Delete PortRange**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

4. Click the **QoS** navigation key to close the navigation tree.

VoIP Gateway

To configure VoIP gateway settings:

1. On the navigation tree, click **VoIP Gateway**.
   Clicking the VoIP Gateway navigation key expands the navigation tree but doesn't display the summary of configurable VoIP Gateway services. You must click **VoIP Gateway**.

   The VoIP Gateway Summary screen appears.

   The VoIP Gateway Summary attributes are:

Attribute	Description
Description	Shows the description of the VoIP gateway.
Version	Shows the version of the VoIP gateway.
Status	Lets users enable, disable, pause, or continue the VoIP gateway service.

2. From the **Status** list box select **Enable** or **Disable**.

3. Press the **Tab** key to save the settings.

VoIP local and remote gateways

To configure VoIP local and remote gateways:

1. On the navigation tree click the **VoIP Gateway** navigation key to expand the navigation tree.

2. On the navigation tree click **Local Gateway**.
   Clicking the Local Gateway navigation key causes the key to disappear. You must click **Local Gateway**.

The VoIP Local Gateway attributes are:

Attribute	Description
Preferred Codecs	Lets users specify the local VoIP gateway used to convert voice to data packets and vice versa. These parameters are always negotiated during call setup with the other VoIP gateway involved in the call. Codecs are negotiated in the order of preference specified here. Refer to the *VoIP Gateway User Guide* for a discussion on these values.
Echo Cancellation	Lets users enable or disable the Echo Cancellation feature in the VoIP calls.
Non-Linear Processing	Lets users enable or disable non-linear processing.
Silence Compression	Lets users enable or disable silence compression.
Fallback to Circuit Switched	Lets users enable or disable fallback to the circuit switched network (PSTN).
Voice Jitter Buffer	Lets users specify the voice jitter buffer size in the range of 20-200. The default setting is 50.
Fax Jitter Buffer	Lets users specify the FAX jitter buffer size in the range of 20-200. The default setting is 50.
Local Gateway IP	Lets users specify the local VoIP gateway to be used as its IP Address while interacting with other VoIP gateways. Since the Enterprise Edge server typically has more than one IP interfaces and more than one IP Address in it, users must choose one that VoIP gateway uses. This address must match the entry for this gateway in the remote gateway table of those VoIP gateways. Ensure this address is reachable to the other gateways via IP.

3. From the **1st Preferred Codecs** list box select the video class.

4. Configure the 2nd through 5th preferred codec selections.

5. From the **Echo Cancellation** list box enable or disable echo cancellation.

6. From the **Non-Linear Processing** list box enable or disable non-linear processing.

7. From the **Silence Compression** list box enable or disable silence compression.

8. From the **Fallback to Circuit-Switched** list box to enable or disable fallback to circuit-switched.

9. In the **Voice Jitter Buffer** box type the voice jitter buffer and press the **Tab** key.

10. In the **Fax Jitter Buffer** box type the appropriate fax jitter buffer and press the **Tab** key.

11. In the **Local Gateway IP** box type the local gateway IP address and press the **Tab** key.

12. Press the **Tab** key save the settings.

To modify VoIP Gateway Remote Gateway services:

1. On the navigation tree, click **Remote Gateway**.
   Clicking the Remote Gateway navigation key causes the key to disappear. You must click **Remote Gateway**.
   The VoIP Remote Gateway screen appears.

To modify a remote gateway:

2. In the **Remote Gateway** table, click the remote gateway you want to modify.

3. On the menu, click **Configuration** and then click **Modify Entry**.
   The Remote Gateway dialog box appears.

The VoIP Remote Gateway attributes are:

Setting	Definition
Name	Lets users specify a logical name for the remote VoIP gateway. This setting is editable only when adding a new gateway entry. While modifying an existing entry, this name can not be changed.
Destination IP	Lets users specify IP Address for the remote VoIP gateway. Fully qualified DNS Name or just host name (where applicable) or IP address in dotted format may be entered here.
QoS Monitor	Lets users enable or disable QoS Monitor for this VoIP gateway.
Transmit Threshold	Lets users specify the transmit threshold that is used while interacting with this VoIP gateway.
Receive Threshold	Lets users specify the receive threshold that is used while interacting with this VoIP gateway.
Gateway Type	Lets users specify the VoIP gateway type. VoiceNet is the only permitted value in Release 1.0.
Destination Digits	Lets users specify the destination digits for this gateway. When the local gateway sees this prefix, it forwards the call to the VoIP gateway at the specified destination IP Address.

4. In the **Name** box type the name of the remote gateway.

5. In the **Destination IP** box type the destination IP address and press the **Tab** key.

6. From the **Qos Monitor** list box enable or disable the QoS.

7. In the **Transmit Threshold** box type the transmit threshold and press the **Tab** key.

8. In the **Receive Threshold** box type the appropriate receive threshold.

9. In the **Destination Digits** box type the destination digits and press the **Tab** key.

10. Click the **Save** button to return to Unified Manager.

To add a remote gateway:

1. On the menu, click **Configuration** and then click **Add Entry**.
   The Remote Gateway dialog box appears.

2. In the **Name** box type the user name.

3. In the **Destination IP** box type the destination IP address.

4. From the **Qos Monitor** list box enable or disable the QoS monitor.

5. In the **Transmit Threshold** box type the transmit threshold and press the **Tab** key.

6. In the **Receive Threshold** box type the receive threshold.

7. In the **Destination Digits** box type the destination digits.

8. Click the **Save** button to return to Unified Manager.

To delete remote gateways:

1. In the **Remote Gateway** table click the remote gateway you want to delete.

2. On the menu, click **Configuration** and then click **Delete Entry**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

4. Click the **VoIP Gateway** navigation key to close the navigation tree.

QoS monitor

To set the QoS monitor:

1. On the navigation tree, click **Services, QoS Monitor**.
   Clicking the QoS Monitor navigation key expands the navigation tree doesn't display the summary of configurable QoS monitor services. You must click **QoS Monitor**.
   The QoS Monitor Summary screen appears.

The QoS Monitor Summary attributes are:

Attribute	Description
Description	Shows the description of the service monitor.
Version	Shows the version of the service monitor.
Status	Lets users enable or disable the service monitor.

2. From the **Status** list box select **enable** or **disable**.

3. Press the **Tab** key to save the settings.

QoS Monitor Mean Opinion Score

To view the QoS Monitor Mean Opinion Score:

1. Click the **Qos Monitor** navigation key.

2. On the navigation tree, click **Mean Opinion Score**.
   Clicking the Mean Opinion Score navigation key causes the key to disappear. You must click **Mean Opinion Score** to view the Mean Opinion Score Services table.

   If you configure or create remote gateways by clicking the Voice Net Remote Gateway navigation key, the mean opinion scores of the connections to these remote gateways, which are a measure of quality of the voice link, while using IP trunk, for each codec type are displayed in the screen. Each configured gateway appears on a separate row.

   Each row consists of the fields for the name of the remote gateway, its IP address, the status of the QoS monitoring for the connection, and the mean opinion scores for each allowed voice codec types and for each direction.

   If the QoS Monitor setting for the remote gateway entry is Disabled the MOS value for the remote gateway is N/A. Also, if the QoS Monitor service is disabled or down for any reason, all MOS values are N/A.

   While MOS values are being shown, they are updated approximately every 50 seconds. To refresh the data, on the menu click **View** and then click **Refresh**.

3. Click the **QoS Monitor** navigation key to close the navigation tree.

Web cache

To configure the web cache settings:

1. On the navigation tree, click **Services, Web Cache**.
   The Web Cache Summary screen appears.

The Web Cache Summary attributes are:

Attribute	Description
Description	Shows the description of the Web Cache server.
Version	Shows the version of the Web Cache server.
Status	Shows the status of the Web Cache server. This setting is read-only. The server always runs to provide support for web-based UIs for Enterprise Edge.
Server Address	Lets users tell the web server what IP address to use for interacting with HTTP clients. Since Enterprise Edge server typically has more than one IP interface and associated IP Address, users can choose this value. This value is automatically set to the IP Address of the first LAN interface and changes when the latter changes. Exercise caution if modifying this value
Cache Mode	Lets users enable or disable the cache-mode of operation.
Cache Size	Lets users specify the maximum size, in KB, of the cache.
Garbage Collection Interval	Lets users specify the interval, in hours, between garbage collection operations on the cache.
Cache Maximum Life	Lets users specify the maximum life, in hours, on the proxy server for the HTTP pages cached in it.
Maximum Server Threads	Lets users specify the number of threads ready to serve HTTP requests in the proxy server.

2. In the **Server Address** box type the server address.
   This setting is automatically set to the LAN interface IP address. Use caution when changing.

3. From the **Cache Mode** list box select **Enable** or **Disable**.

4. In the **Cache Size** box type the cache size in KB.

5. In the **Garbage Collection Interval** box type the interval in hours.

6. In the **Cache Maximum Life** box type the cache maximum in hours.

7. In the **Maximum Server Threads** box type the number of threads.

8. Press the **Tab** key to save the settings.

Net Link Manager

To configure Net Link Manager settings:

1. On the navigation tree click **Services, Net Link Manager**.
   The Net Link Manager Summary screen appears.

The Net Link Manager Summary screen attributes are:

Attribute	Description
Description	Shows a description of the Net Link Manager.
Version	Shows the version number of the subsystem.
Status	Shows the status of the Net Link Manager. The Net Link Manager is always running and cannot be disabled by the user.
Next Hop on Primary Link	Lets users specify the IP address in a valid dot format of the next hop router which is typically the remote router of the primary WAN data link.
Up Poll Interval	Lets users set the polling interval, in seconds, while the primary WAN data link is operational.
Down Poll Interval	Lets users set the polling interval, in seconds, while the primary WAN data link is down, and the dial-up data link is operational.
Switch Over Delay	Lets users specify the interval, in seconds, that Net Link Manager waits for before switching the network link after it notices that the primary WAN link has come up again. This delay lets the router on the other end of the primary link recognize that the link has come up and adjust routing table accordingly. Typically this is set to the RIP Route Announcement Interval of 30 seconds.

2. From the **Status** list box select enable or disable.

3. In the **Next Hop on Primary Link** box type the "next hop."
   This address is used by NetLink Manager to add a default route in the Enterprise Edge server. If this address is unreachable, NetLink Manager dials the backup link and changes the default route.

4. In the **Up Poll Interval** box type the up poll interval in seconds.
   The up poll interval is the interval between successive pings when the next hop in primary link is available. Use a relatively larger value to save bandwidth.

5. In the **Down Poll Interval** box type the down poll interval in seconds.
   The down poll interval is used to ping the next hop on primary link when it is recognized as unreachable. Use a smaller interval for faster recovery.

6. In the **Switch Over Delay** box type the switch over delay in seconds.

7. Press the **Tab** key to save the settings.

Call Detail Recording

To view Call Detail Recording settings:

1. On the navigation tree click **Services, Call Detail Recording**.
   Clicking the Call Detail Recording navigation key expands the navigation tree but doesn't display the read only summary. You must click **Call Detail Recording**.
   The read only Call Detail Recording Summary screen appears.

The Call Detail Recording Summary screen attributes are:

Attribute	Description
Name	Shows the component name, which is CDR.
Status	Shows the status of the component.
Version	Shows the version of the component.
Description	Shows a description of the component.

Report parameters

To configure the Call Detail Recording report parameters:

1. On the navigation tree, click the Call Detail Recording navigation key to expand the navigation tree.

2. Click **Report Params** from the navigation tree.
   Clicking the Report Parameters navigation key causes the key to disappear. You must click **Report Params**.
   The Report Parameters screen appears.

The Call Detail Recording report parameters are:

Attribute	Description
Format	Lets user specify the record format from: SL-1 Norstar The default format is SL-1.
Report Type	Lets users select the report type from: Standard: Standard call information only CLID: Standard call information with CLID records Real time: Report real time call information for incoming calls only (available only when Norstar format is selected) All: Report standard call information with CLID records and real time call information (available only when Norstar format is selected) The default report type is Standard.
Language	Lets users select the language from: English French The default language is English
Report Filter	Lets users select the report filter type from: Outgoing: Report only outgoing calls. Incoming calls are not reported. Account Code: Reports only calls with account code stamped. Prefix: Report only calls with digits matched that long distance code in the prefix table. All: Reports all calls The default report filter is All.
Feature Code F9	Lets users specify the Feature Code F9 setting.

3. From the **Format** list box select the format.
4. From the **Report Type** list box select the report type.
5. Click the **Language** list box select the language.
6. From the **Report Filter** list box select the report filter.
7. From the **Feature Code F9** box select the feature code.
8. Press the **Tab** key to save the settings.

To configure commit and clip files:

1. On the menu, click **Configuration** and then click **Commit**.

Report options

To set Call Detail Recording report options:

1. On the navigation tree, click **Services, Call Detail Recording, Report Options**.
   Clicking the Report Options navigation key causes the key to disappear. You must click **Report Options**.
   The Report Options screen appears.

The Call Detail Recording report options are:

Attribute	Description
Date Format	Lets users specify the date format on voice mails recorded from: MM/DD/YY DD/MM/YY YY/MM/DD The default date format is MM/DD/YY.
Header Format	Lets users specify the header format for the recorded messages from: Line/Station: always reports the Line number first followed by the station number. Source/Destination: reports the source of the call followed by the destination of call. Incoming calls are reported in Line/Station format. Outgoing calls are reported in Station/Line format. The default header format is Line/Station format. This parameter affects only the Norstar record format.

DNIS Info	Lets users enable and disable reporting Dialed Number Information Service (DNIS) digits. The default DNIS Info is Enabled This parameter affects only the Norstar record format. Not all trunks support DNIS.
Connect Char	Lets users enable and disable inserting "!" between digits dialed and after the call is connected. The default connect char is Disabled.

2. From the **Date Format** list box select a date format.

3. From the **Header Format** list box select a header format.

4. From the **DNIS Info** list box select enable or disable.

5. From the **Connection Character** list box select a connection character.

6. Press the **Tab** key to save the settings.

Market parameters

To set the Call Detail Recording market parameters:

1. On the navigation tree, select **Services, Call Detail Recording, Market Params**.
   Clicking the Market Parameters navigation key causes the key to disappear. You must click **Market Params**.
   The Call Detail Recording Market Parameters screen appears.

The Call Detail Recording market parameters are:

Attribute	Description
CLID with Name	Lets users enable and disable reporting the CLID Name of the call. This parameter affects only the Norstar record format. Not all trunks support CLID Name. The default NameCLID is Enabled.
Long CLID Support	Lets users enable and disable supporting the long CLID digit reporting. This parameter is very market specific. Do not change the default unless the trunk supports this feature. The default Long CLID is Disabled.
CLID with Call Type	Lets users enable and disable reporting the call type (Long distant or Unknown). This parameter affects only the Norstar record format. Do not change the default unless the trunk supports this feature. The default call type is Enabled.
Support Call Charge	Lets users enable and disable supporting the call charge reporting. This parameter is very market specific. Do not change the default unless the trunk supports this feature. The default call charge is Disabled.

Answer Supervision	Lets users enable and disable using Answer Supervision to identify far-end answered outgoing calls. This parameter is very market specific. Do not change the default unless the trunk supports this feature. The default ans supervision is Disabled.
Call Filter Duration	Lets users enter the call filter duration. The range is 1-30.

2. From the **CLID with Name** list box enable or disable Name CLID.

3. In the **Long CLID Support** list box enable or disable Long CLID Support.

4. From the **CLID with Call Type** list box enable or disable CLID with Call Type.

5. From the **Support Call Charge** list box enable or disable Call Charge Support.

6. From the **Answer Supervision** list box enable or disable answer supervision.

7. In the **Call Filter Duration** box, enter the call filter duration, from 1-30.

8. Press the **Tab** key to save the settings.

PreFix Bins

The prefix bins let users enter the long distance call prefixes in conjunction with the report filter option.

To set the Call Detail Recording PreFix Bins settings:

1. On the navigation tree, select **Services, Call Detail Recording, PreFix Bins**. Clicking the PreFix Bins navigation key causes the key to disappear. You must click **PreFix Bins**.
   The PreFix Bin Settings screen appears, where you can define up to eight prefixes.

2. In the **PreFix Bin Settings** boxes type the appropriate prefixes.

3. Press the **Tab** key to save the settings.

Access Bin Settings

To configure Call Detail Recording access bin settings:

1. On the navigation tree, select **Services, Call Detail Recording, Access Bin Settings**.
   Clicking the Access Bin Settings navigation key causes the key to disappear. You must click **Access Bin Settings**.
   The Access Bin Settings and Suppress Length Settings screens appear.

The Access Bin Settings attributes are:

Attribute	Description
Access Setting	Lets users enter the secondary call provider call prefix digits.
Suppress Setting	Lets users enter the length of personal identification digits to suppress.

2. In the **Access** and **Suppress** boxes type the appropriate access and suppress settings.
   You can define up to five settings for each.

3. Press the **Tab** key save the settings.

4. Click the Call Detail Recording navigation key to close the navigation tree.

TAPI Service Provider

To configure TAPI Service Provider settings:

1. On the navigation tree, select **Services, TAPI Service Provider**.
   Clicking the TAPI Service Provider navigation key causes the key to disappear, but doesn't show the read-only settings. You must click **TAPI Service Provider**.
   TAPI Service Provider Settings and configurable Station List screens appear.

   TAPI Service Provider Settings are read-only; however, you can add and delete station in the Station List. The TAPI Service Provider attributes are:

Attribute	Description
Status	Shows the current status of the TSP (telephony service provider) as reported by the TSP software. The possible values are: Unknown In Service Not In Service Initializing In KSU Admin These strings are presented in English, French, or Spanish, depending on the software settings. The default value is Unknown and the typical value is In Service.

Attribute	Description
Description	Shows the description of TSP.
Version	Shows the TSP version.
Station Licenses	Shows the number of sets that are licensed to be controlled through the TSP. This is a numeric value or the text string Unlimited or Maximum. The station licenses can not be modified on this page but are changed by adding a keycode through the Software Keys page. The string Unlimited is presented in English, French, or Spanish. The default value is 2.
Station	Lets users add an internal phone number on the Enterprise Edge system. Users can add as many entries as there are licenses have been granted. The default is no entries in the Station List. List elements are added and deleted through the Configuration menu items.

To add a station:

1. On the menu click **Configuration** and then click **Add Station to List**. The Station List dialog box appears.

2. In the station box type the station information.

3. Click the **Save** button to return to Unified Manager.

To delete a station:

1. Select the station from the Station List that you want to delete.

2. On the menu click **Configuration** and then click **Remove Station from List**. A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

Console Service

To configure Console Service attributes:

1. On the navigation tree, select **Services, Console Service**. The Console Service Summary and Licensing screens appear.

2. Configure the Console Service Summary and Licensing attributes according to the following table:

Attribute	Description
Status	Lets users specify the status of the Attendant Console. The options are: EnableManual EnableAuto Start Stop

Attribute	Description
Version	Lists the version of the Attendant Console. This attribute is read-only.
Description	Provides a description of the Attendant Console. This attribute is read-only.
Licensed Seats	Lists the number of licensed seats. This attribute is read-only.
Used Seats	Lists the number of used seats. This attribute is read-only.

Server Configuration

To configure the Server Configuration attributes for the Attendant Console:

1. From the navigation tree, select **Services, Console Service, Server Configuration**.
   The Voice Mail Port and Station Discovery screens appear.

2. Configure the Voice Mail Port and Station Discovery attributes according to the following table:

Attribute	Description
Voice Mail Pilot Extension	Lets users specify the default voice mail extension for the system. Specify an extension number for the voice mail system.
Rediscover Station List on next restart	Lets users specify whether the system tries to communicate with all possible destination numbers to check for their status. Exercise caution before enabling this option as it can take up to 30 minutes to complete.

General Information

To view the General Information attributes for the Attendant Console:

1. From the navigation tree, select **Services, Console Service, General Information**.
   The General Information screen appears. This screen is read-only.

2. View the general information, which the following table describes:

Attribute	Description
Access Version	Lists the access version of the Attendant Console.
Attendant Console Server Version	Lists the attendant console server version.
Switch Hardware Version	Lists the version of the switch hardware.
Switch Software Version	Lists the version of the switch software.
Attendant Console Server Manager	Lists the version of the attendant console server manager.

Diagnostic Logging

To configure the Diagnostic Logging attributes:

1. From the navigation tree, select **Services, Console Service, Diagnostic Logging**.
   The Diagnostic Logging screen appears.

2. Configure the Diagnostic Logging attributes according to the following table:

Attribute	Description
Log Detail Level	Lets users specify the debug level. Any value between 0 and 20 is acceptable. The typical setting is 5.
Log To file	Lets users enable logging to the file. If enabled, it creates a file called ConsoleService.log on the file system.
Log CP Events Log Device Events Log Response Events Log Session Events Log System Events	Lets users enable events, including various types of events in the log file generated.

Alarm Service

To configure Alarm Service settings:

1. On the navigation tree select **Services, Alarm Service**. Clicking the Alarm Service navigation key causes the key to disappear. You must click **Alarm Service**.
   The Alarm Service Summary screen appears.

The Alarm Service Summary screen attributes are:

Attribute	Description
Descriptions	Shows a description of the alarm service.
Version	Shows the version of the alarm service.
Status	Lets users enable or disable the alarm service.

2. From the **Status** list box enable or disable alarm service.

3. Press the **Tab** key to save the settings.

Voice Mail

To configure Voice Mail services settings:

1. On the navigation tree select **Services, Voice Mail**.
   Clicking the Voice Mail navigation key causes the key to disappear. You must click **Voice Mail**.
   The Voice Mail Summary screen appears.

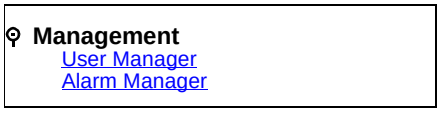
The Voice Mail Summary screen attributes are read-only. The attributes are:

Attribute	Description
Name	Shows the name of the component.
Status	Shows the status of the voice mail service.
Version	Shows the version of the voice mail service.
Description	Shows the description of the voice mail service.

2. Click the **Services** navigation key to close the navigation tree.

Configuring Management Settings 8

The following shows the programming map for **Management**:



In the Enterprise Edge Unified Manager, **Management** enables you to manage user and alarm settings. Within **Management**, you have the following options:

- User Manager, which brings up the User Profile screen. Here you can add, modify, and delete user names along with their passwords and access privileges.
- Alarm Manager, which brings up the Alarm Database and SNMP Trap screens. Here you can modify the collection parameters of the Alarm Database. You can also enable or disable the sending of various SNMP traps.

User Manager

When Enterprise Edge ships, the following user IDs are available:

- manager: administrator user, with "manager" as the default password
- user: read-only user, with "user" as the default password
- supervisor: administrator user, with "super" as the default password

Note: After installation, change the password for all administrator users or delete them after creating your own administrator users.

To access the User Manager, select **Management, User Manager** from the navigation tree. The User Profile screen appears. The attributes on the User Profile screen are:

Attribute	Description
User Name	Lets users specify the user name while adding a new user. While modifying an existing user profile, this field is read-only. This attribute is case sensitive and cannot exceed 50 characters in length.
Password	Lets users specify the password for the user. This attribute is case sensitive and cannot exceed 15 characters in length.
Confirmed Password	Lets users confirm the modified password. This attribute must match the Password attribute.
Privilege	Lets users specify what privileges the user has in administering the Enterprise Edge server. The options are: READ-ONLY: Lets users view attributes, but not alter them. READ-WRITE: Lets users view and change attributes.

To add user profiles:

1. Click any line in the **User Profile** table.

2. On the menu click **Configuration** and then click **Add User**.
   The User Profile dialog box appears.

3. In the **User Name** box type the user name.

4. In the **Password** box type the password.

5. In the **Confirmed Password** box type the password again.

6. From the **Privilege** list box select the appropriate user privilege.

7. Click the **Save** button to return to Unified Manager.

   Note: Maintain only one user profile with administrative privileges and with a few people allowed to use it. Multiple users logging on to Enterprise Edge from different client stations through the administrator account can causes inconsistent or wrong configuration. There is no security within Enterprise Edge to prevent this.

To modify user profiles:

1. In the **User Profile** table, click the user profile you want to modify.

2. On the menu click **Configuration** and then click **Modify User**.
   The User Profile dialog box appears.

3. In the **Password** box type the new password, if necessary.

4. In the **Confirmed Password** box retype the password.

5. From the **Privilege** list box select the appropriate user privilege.

6. Click the **Save** button to return to Unified Manager.

To delete user profiles:

1. In the **User Profile** table click the profile you want to delete.

2. On the menu click **Configuration** and then click **Delete User**.
   A message appears that asks you to confirm the deletion.

3. Click the **Yes** button to confirm the deletion and return to Unified Manager.

Alarm Manager

Enterprise Edge provides real-time information about what is occurring within the Enterprise Edge system. The Alarm Manager enables you to manage the collection and storage of this information. In the Alarm Manager, you can set various collection parameters for the Alarm Database. You can also enable or disable the sending of all or various types of SNMP traps.

To access the Alarm Manager, select **Management, Alarm Manager** from the navigation tree. The Alarm Database and SNMP Trap screens appear. The following table describes the Alarm Database and SNMP Trap attributes. Set these attributes according to the information that the table provides.

Attribute	Description
MaxNumRec	Shows the maximum number of records that the alarm database stores. This attribute is READ-ONLY at this time.
DiscardTime	Shows the discard time, in seconds, for repeat alarms. If the same alarm happens in this interval, it is discarded. This attribute is READ-ONLY at this time.
KeptTime	Shows the number of days that the alarm database keeps alarm records.
ResyncTime	Shows the resynchronization time, in seconds. Alarm service re-synchronizes with the event log at this interval. A value of 0 disables resynchronization.
TrapsEnabled	Lets users enable or disable sending SNMP traps when a new event arrives in the event log.
EventInfo Enabled	Lets users enable or disable sending SNMP traps when an 'Information' event arrives in the event log.
EventWarning Enabled	Lets users enable or disable sending SNMP traps when a 'Warning' event arrives in the event log.
EventError Enabled	Lets users enable or disable sending SNMP traps when an 'Error' event arrives in the event log.
ScrExclusion List	Lets users specify a comma-separated list of event sources whose events are not reported as SNMP traps. Depending upon the network and user environment, a component in Enterprise Edge can generate events of no significance to you at regular intervals. Adding that event's source name here prevents the generation of SNMP traps for that event.

To view the fault alarms, refer to Viewing system performance and fault alarms on page 283.

Maintenance 9

A maintenance session helps you diagnose problems that may occasionally arise within the Enterprise Edge system. Maintenance sessions also allow you to determine how the system will deal with T1 digital lines, and provides a means for provisioning and testing digital lines. Perform your maintenance programming in the Unified Manager, under the Maintenance selection. For more information on maintenance procedures refer to:

- System startup on page 233
- Warm reset on page 234
- Backup and restore on page 234
- Enterprise Edge system diagnostics and utilities on page 241
- Maintenance programming for telephony resources on page 253

For information on hunt group and call-by-call usage metrics, refer to Metrics on page 279.

For information on physically moving telephones, refer to Moving telephones on page 279.

System startup

A system startup replaces any existing telephony programming with the default programming.

1. Choose **Resources**, **Telephony**, **Maintenance**.

   The Configuration menu is enabled.

2. Access the Configuration menu and click **System startup**.

   The system displays a dialog box with two parameters; template and start dn.

3. Select one of two templates from the template drop-down menu; PBX or DID.

4. Type any valid value in the **start dn** box. The box displays the current value.

5. Click **OK** to apply these changes.

   The system displays a warning that the telephone system will restart and that default programming values will be restored.

Warm reset

A warm reset restores the system but does not affect the current telephony programming.

1. Choose **Resources**, **Telephony**, **Maintenance**.

   The Configuration menu option is enabled.

2. Access the Configuration menu and click **Warm reset**.

   The system displays a warning that all active calls will be dropped.

3. Click **OK** to continue.

Backup and restore

- Backup, restore, upgrade utility (BRU) for Enterprise Edge system on page 234
- Backup and restore telephony programming on page 237

Backup, restore, upgrade utility (BRU) for Enterprise Edge system

The BRU utility manages local, remote and Web-enabled Enterprise Edge software. BRU works with *.xml* files to perform step-by-step backup, restore or upgrade of the full Enterprise Edge system or selected components. After you select the desired components, BRU creates a ready-to-run Windows NT script file that can be executed immediately or at a scheduled time and date.

You launch the BRU utility after starting a virtual network computing (VNC) session. The VNC desktop sharing utility supplied with Enterprise Edge allows you to access the desktop of the Enterprise Edge server from another computer. For more information, refer to *Enterprise Edge Installation and Maintenance Guide*.

BRU provides additional functionality that complements the Unified Manager telephony programming backup and restore features.

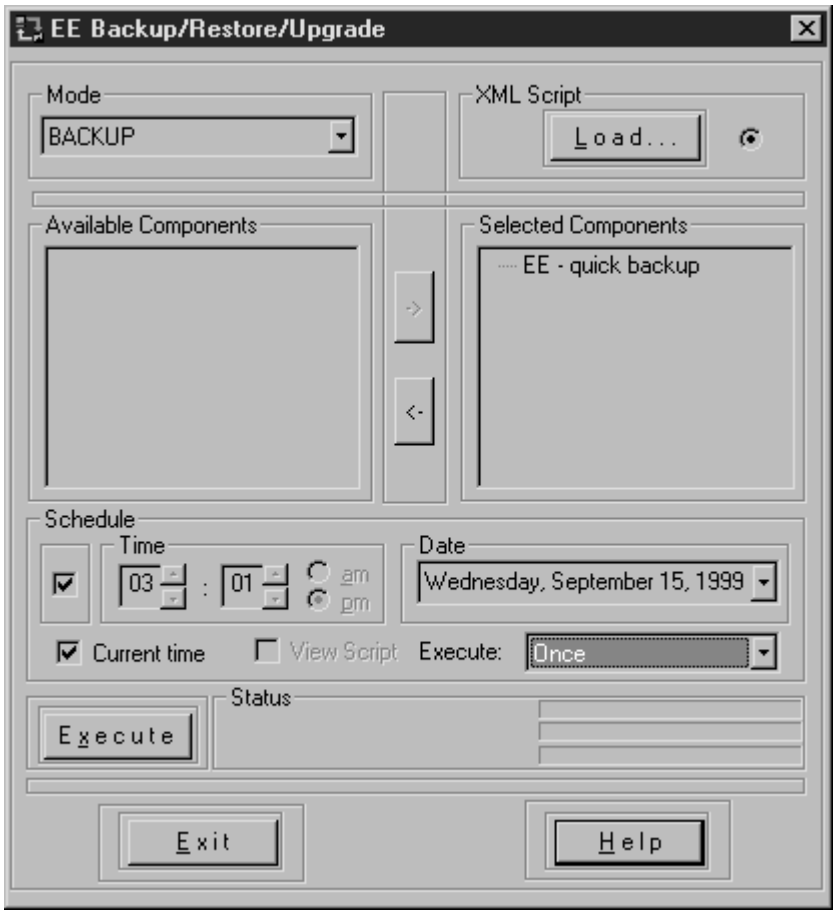
The backup and restore tool in the Unified Manager allows you to back up your system programming or retrieve a complete copy of all or selected programming information from the Enterprise Edge system. This information is backed up on the Enterprise Edge system ‘D’ drive. If one of the files stored on your Enterprise Edge server drive becomes corrupted, you can successfully restore the programming information.

BRU is used to backup the system registry and customer data stored by default on the Enterprise Edge ‘D’ drive. The backup can be stored on any network accessible drive.

Telephony programming is backed up to the D: drive prior to performing a backup with BRU.

For a brief description of telephony backup and restore programming in the Unified Manager see Backup and restore telephony programming on page 237.

The BRU window



Building Windows NT script files

BRU creates a Windows NT *.cmd* file from the information retrieved from the *.xml* file and data from user input. The assembled *.cmd* file is then executed. In order to create a backup, restore or upgrade script, BRU must first load the corresponding *.xml* file.

Each *.xml* file contains a top level section that lists the main sections in the *.xml* file with for example, tasks such as BACKUP, RESTORE, or UPGRADE. For each of these tasks there is a list of available components.

The *.cmd* file is built from selections from the list of available components. Once the component is in the Selected Components window, BRU reads the instructions for this component and writes the *.cmd* file. BRU can execute the file immediately or at a specified time and date on a Once, Daily, Weekly, or Monthly schedule.

To create and execute a script file:

1. Initiate a telnet session to access the Enterprise Edge desktop and start the remote desktop sharing service called VNC, by typing ‘net start winvnc’.

2. Login to the server with your browser and specify port 5800.

3. On the desktop click **Start**, **Programs**, **Nortel Networks**.

4. Double-click the BRU icon to run the program.

5. Click **Load** to load an *.xml* script file.

6. Choose an *.xml* file from the Open dialog box.

7. Click **Open**.

8. Select a mode from the Mode list box.

9. Select an available component from the Available Components box.

10. Click the right arrow button to move the component to the Selected Components box.

11. Click **Execute** to run the file immediately.

    or

12. Select the Current Time checkbox to set the time of execution based on the system time.

13. Select or type the execution date in the Date list box.

14. Click **Execute**.

    or

15. Select the Schedule check box to enable the Execute list box.

16. Select Once, Daily, Weekly, or Monthly from the Execute list box.

17. Select or type the execution date in the Date list box.

18. Click **Execute**.

Note: The current version of BRU allows scheduling single executions of the script file on a given date. Repetitive scheduled execution capability is not available.

Note: When in update mode, BRU performs a silent mode auto uninstall of the specified software component if the *.xml* file contains an uninstall token and if the system registry contains uninstall information for the component. If the component information is not available, BRU runs an interactive version of the uninstall script.

Backup and restore telephony programming

The Backup and Restore menu option, in the Unified Manager, allows you to back up your telephony programming or retrieve a complete copy of all or selected programming information from the Enterprise Edge system.

If one of the files stored on your server becomes corrupted, you cannot successfully restore the programming information. Equip your server with an application that protects files from computer viruses and performs file backup and encryption.

The Backup and Restore tool stores up to two different copies of system programming:

- Current copy: this version contains the system programming at the time of the last backup. The current file is named Fnvram.NEW (current copy of system programming)
- Archive copy: this version contains the Enterprise Edge system programming at the time of the second last backup. It was the current copy until it was replaced by the most recent backup. The archive file is named Fnvram.OLD (archive copy of system programming)

You cannot change the file names of the programming backup. If you need to create alternate versions of the files, create additional folders. Backups are treated like an assembly line. When a successful backup is performed, the information stored in the current version is moved to the archive version.

Refer to the following procedures for more information:

- Performing a backup on page 238
- Performing a restore on page 238
- Stopping a backup on page 240
- Stopping a restore on page 240

Note: The Backup, Restore, Upgrade utility (BRU) provides additional functionality that complements the Unified Manager telephony programming backup and restore features. BRU works with *.xml* files to perform step-by-step backup, restore or upgrade of the full Enterprise Edge system or selected components. For more information, refer to Backup, restore, upgrade utility (BRU) for Enterprise Edge system on page 234.

Performing a backup

When you perform a backup, the telephony component of your system slows down, but remains completely operational. Backups keep your server working for a period of time therefore schedule backups for when you don't need your server for other tasks.

Use the following procedure to perform a backup.

1. Verify that you are using the correct backup file for your system.

   If you attempt to use an incompatible file for a restore, it will cause a warm start of the Enterprise Edge system (a restart where no programming is lost).

2. Start the Backup and Restore tool by choosing **Resources**, **Telephony**.

   The **Tools** menu option is enabled.

3. Click **Tools**, **Backup**.

   A confirmation dialog is displayed, asking if you wish to start now.

4. Click **Yes** to start.

   When a backup is in progress, the text shows the current action and the file name. For example, "Backing up System Programming into file Fnvram.new." When a backup is in progress, a bar graph shows the rough percentage of the action that is complete. It does not appear unless a backup or restore is occurring.

Note: When a backup is in progress, you can click Cancel to discontinue the operation. For more information, refer to Stopping a backup on page 240. When a backup is in progress, you can also start another backup.

5. When the backup is complete, click **Done**.

   The Backup and Restore dialog box closes.

Performing a restore

The Restore feature allows you to overwrite existing programming, or to upgrade the system. When you perform a restore, the telephony component of your system is non-operational and call processing is suspended. Perform restores during non-business hours, and warn users that the Enterprise Edge system will be out of service. Schedule restores for a time when you don't need your server for other tasks.

When you run a restore, all of the sets are put in maintenance mode. Programming data from your server's hard disk or other data storage medium is then loaded into the system's memory. After the data is loaded, the Backup and Restore tool takes the sets out of maintenance mode by initiating a warm start. A warm start restarts the Enterprise Edge system with all its programming intact, including any changes you have made.

Use the following procedure to perform a restore...

A restore overwrites existing programming
You cannot recover Enterprise Edge system programming that has been overwritten.

If a restore fails, the system initiates a cold start
If a restore fails to complete due to an error, the system will initiate a cold start. This means that all programming will be lost, and all programming settings will be returned to the factory defaults.

Ensure the restore is completed successfully
A restore replaces all existing programming for a Enterprise Edge system. A failed restore can shut down a Enterprise Edge system and telephone service to a site, so it is important to ensure the restore is completed successfully.

1. Start the Backup and Restore tool by choosing **Resources**, **Telephony**.

   The **Tools** menu option is enabled.

2. Click **Tools**, **Restore**.

Note: If you restore any programming which has been enabled by software keys, you may have to re-enter the keys after the restore.

A confirmation dialog is displayed, asking if you wish to start now.

3. Click **Yes** to start.

   When you initiate a restore, there is a period of a minute or longer while the restore action is initiated. When a restore is in progress, the text shows the current action and the file name. For example, "Restoring System Programming into file Fnvram.new." The system also displays the percentage of programming that has been restored. It does not appear unless a restore is occurring.

   When the restore is complete, the system automatically restarts.

Note: When a restore is in progress, you can click **Cancel** to discontinue the operation. For more information, refer to Stopping a restore on page 240.

4. Verify the system is working properly once the restore is complete.

Stopping a backup

1. When the restore is in progress, click **Cancel** to discontinue the operation.

   The **Close Application** dialog box appears. The backup continues behind the dialog box until you respond.

2. Click **Yes** to stop the backup.

   If you click **No**, the backup will continue.

Stopping a restore

If you stop a restore, you must perform another, successful restore or the system will initiate a cold start. This means all programming will be lost and all settings will return to the factory defaults.

1. When the restore is in progress, click **Stop** to discontinue the operation.

   The **Stop Restore** dialog box appears.

2. Click **Yes** to stop the restore action.

   If you click **No**, the restore action continues.

3. If you select **Yes**, the **Cold Start Warning** dialog box appears. It tells you that the system will initiate a cold start. You can only click **Exit Application.**

4. Click **Exit Application**.

Enterprise Edge system diagnostics and utilities

This section includes information Enterprise Edge diagnostics and utilities including:

- Uploading System Settings
- Downloading System Settings
- Enterprise Edge Performance Utility
- Error Messages
- MIB II Information

Saving System Settings

Enterprise Edge allows you to save the customized system settings for:

- Archival and backup purposes
- Downloading system settings to multiple Enterprise Edge units

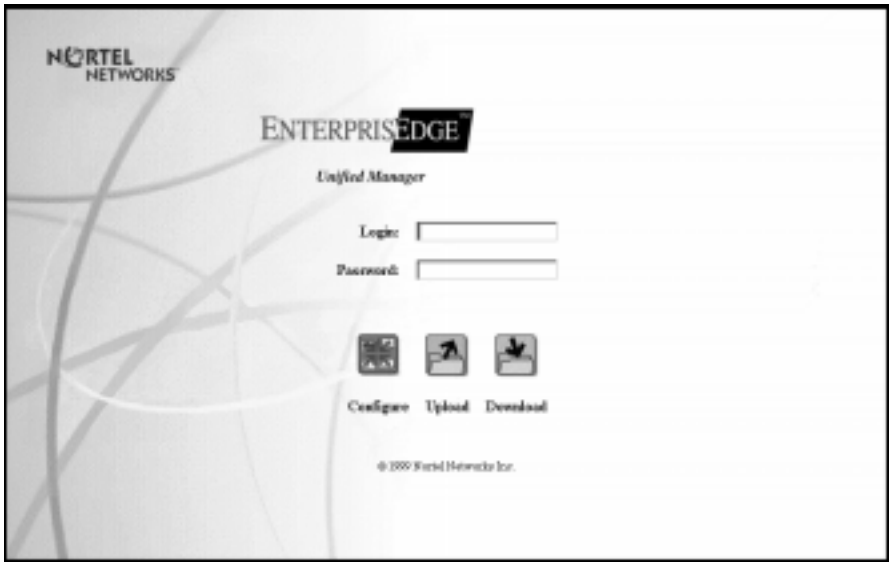
For example, you can use the download or upload feature to configure several Enterprise Edge servers by downloading definitions and uploading them onto new machines. This method of uploading definitions saves configuration time and can be used for archival and backup purposes.

Note: The upload feature is not supported in release 1.

Downloading System Settings

To download files:

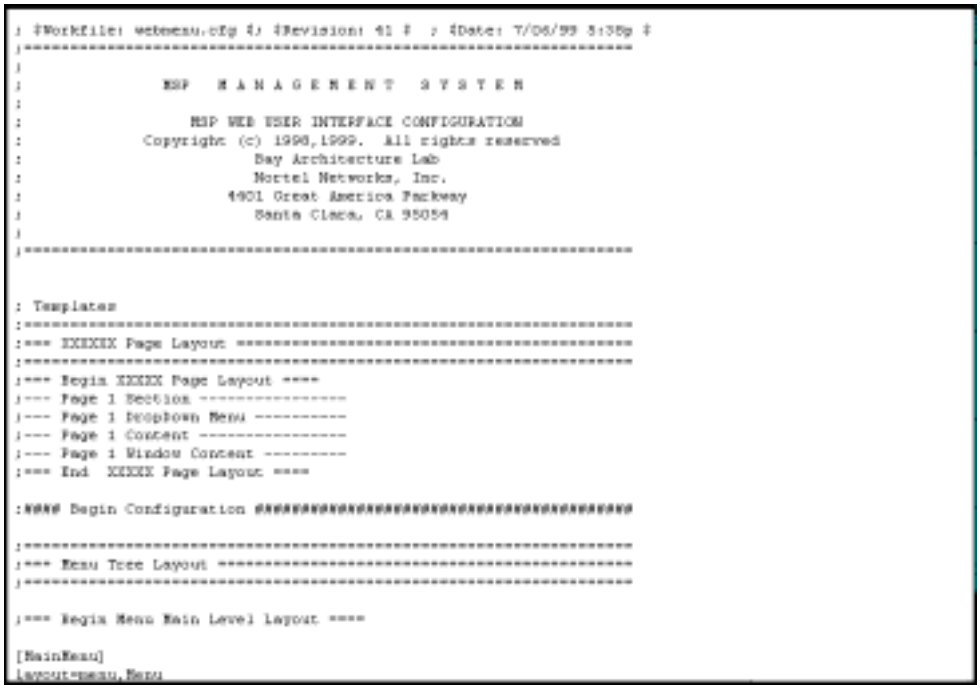
1. On the log on screen, click the **Download** button.



The download screen appears.

2. Select the underlined file and a download screens appears for the user to copy the file from the Enterprise Edge server to the user machine.

   The configuration files that you can download include the web user interface configuration and the subsystem configuration.



```
; $Workfile: webmenu.cfg $; $Revision: 41 $  ; $Date: 7/06/99 5:35p $
;=================================================================
;
;               MSP   M A N A G E M E N T   S Y S T E M
;
;                  MSP WEB USER INTERFACE CONFIGURATION
;             Copyright (c) 1998,1999.  All rights reserved
;                        Bay Architecture Lab
;                        Nortel Networks, Inc.
;                      4401 Great America Parkway
;                        Santa Clara, CA 95054
;
;=================================================================


; Templates
;=================================================================
;=== XXXXXX Page Layout ==========================================
;=================================================================
;=== Begin XXXXX Page Layout ====
;--- Page 1 Section ---------------
;--- Page 1 Dropdown Menu ----------
;--- Page 1 Content ---------------
;--- Page 1 Window Content ---------
;=== End  XXXXX Page Layout ====

;#### Begin Configuration ##########################################

;=================================================================
;=== Menu Tree Layout ============================================
;=================================================================

;=== Begin Menu Main Level Layout ====

[MainMenu]
Layout=menu,Menu
```

```
;$Header: /Management/Code/utils/config/subsys.cfg 9D    8/05/99 3:28p Salve $

[ALL]
Provider=MSPSYS.DLL
Get=GetComponents
Set=SetModifiedTime

;no Set Method
;no Verify Method
;no Prepare Method
;no Apply Method

Fields=LastModified
;Components=SYSTEM,IP,DNS,DHCP,QoS,UserMgr,VOIP,QoSMon,VoCoder,VGtw,MOS,QMON,MSC,MscRcs,MscTel,Router,SNM
Components=SYSTEM,IP,DNS,DHCP,QoS,UserMgr,VOIP,QoSMon,VoCoder,VGtw,MOS,QMON,MSC,MscRcs,MscTel,Router,SNMP

Resources=LAN,WAN,MSC,MscRcs,MscTel,PRI
Services=DHCP,DNS,QoS,Router,SNMP,VOIP,QMON,Apache,WanLinkMgr,CDR,TSP,VoiceService,AlarmSvc

;Components=SYSTEM,IP,DNS,DHCP,WINS,ROUTER

[ClassMap]

;all sections are matched for only first 'n' characters, case-sensitive
CfgElement=ALL,SYSTEM,REBOOT,IP,IP-LAN,DNS,Router,Apache,
DynaFldElement=QoS,SNMP,IP-WAN,BTR-,UserMgr,VOIP,VGtw,MOS,MscRcs,MscTel,AlarmMgr,VoCoder,CDR,TSP,AlarmSvc
DhcpElement=DHCP

[DEFAULT]
;===Begin Attribute Setting ======================================
DEFAULTLABEL=Label,r,t,s,50,none
DEFSTAT=Disabled,rw,d,s,20,Enabled|Disabled
DEFSTAT2=Disabled,rw,d,s,20,Enabled|Disabled|Paused|Continue
DEFDESCR=none,r,t,s,100,none
DEFVER=none,r,t,s,50,none
;===End   Attribute Setting ======================================
```

Graphs and tables

Enterprise Edge provides detailed performance information for the system and its components. The statistics are shown in charts or tables. If a performance display is active, it is automatically updated with real-time performance information in time increments that you set.

Note: Generating statistics puts a significant workload on the Enterprise Edge server CPU, connecting network, and web client. Exercise caution when running statistics for long durations.

Generating Statistics

Enterprise Edge provides statistical information on Enterprise Edge throughput and other performance-related information. The data is formatted in a chart or table format.

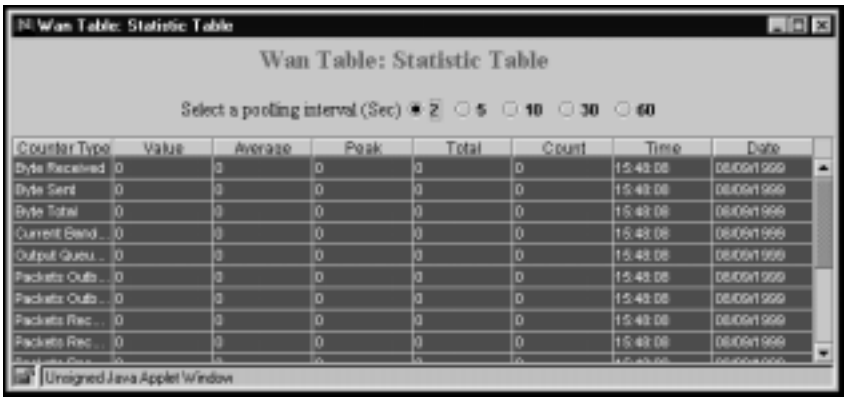
To generate statistics:

1. Select the appropriate item in the navigation tree.
2. Select **Performance** from the menu and select the appropriate command to display statistical information.z
3. The chart or table appears.

Statistical Chart

The following is the same information in table format.

Statistical Table



Sample Rate

You can set the sample rate by selecting the buttons on the statistical display. The polling intervals include 2, 5, 10, 30 and 60 seconds.

Error Messages

Messages appear if there is a system or processing error. The messages include two parts: the error string and the error number.

The error string includes the error description and the context of the error.

The error number is a three-part number that uniquely identifies the error. Be sure to note the error number when communicating with TSC to resolve the problem.

User Actions

Some Enterprise Edge errors are caused by a wrong parameter value. For these errors, the recommended action resolves the problem. Other possible errors are caused by an internal transition of states that puts the system and the user in an error condition. In this event, assistance from TSC is required to resolve the problem.

Note: Any Enterprise Edge errors that are not listed in this manual are advanced and require assistance from TSC for resolution.

Errors List

In the following list, in cases where multiple errors can happen in a particular context, a wild-card representation is used.

Error Number	Description	Action
2.5.4	This is an invalid data error. There was an error in setting system date. Reason: The date, month or year component contains a zero or negative value.	Provide the correct date value.

2.xx.4	These are various errors related to an error in setting system date Reason: The system rejected the date for various reasons. The reasons could be that it is beyond the range of dates supported. For example, 01/01/0001 is invalid date	
2.5.6	This is an invalid data error. There was an error in setting system time. Reason: The hour or minute component contains a negative value.	Provide the correct date value.
2.xx.6	These are various errors related to an error in setting system time	Correct the error in the time format.
2.5.8	This is an invalid data error. There was an error in setting system name. Reason: The system name does not follow the standard conventions.	Make sure that your system name does not contain any special characters in the name (hyphens are allowed, in addition to letters and digits), and that it does not exceed 15 characters in length.
5.4.59	This is an invalid configuration error. There was an error getting or setting DHCP parameters. Reason: You were adding an IP Address Range and/or Excluded Address Range and the first field you entered had a wrong key value. In the dialog boxes that appear to add the entries, the first field is a key that should match certain naming conventions. The conventions are given the label to those fields.	Follow the conventions given on the dialog boxes. For IP Address Ranges, use keys like 'Rxx' and for Excluded Address Ranges, use keys like 'Exx'
5.5.39	This is an invalid data value. There are invalid values for the new excluded address range. Reason: The IP Address values specified for the range are not correct. At present, each component in IP address specified in dotted format should be in the range 0-255, not including the boundary values.	Fix the value. If your IP Address range contains more than 255 addresses in it and you need to exclude a range that ends with 255 or starts with. 0, use the next upper or lower value to avoid specifying this value.
5.5.40	This is an invalid data value. There are missing values in the new excluded address range. Reason: Data for each excluded address entry should include two values - one for the start and the other for end. This error happens if one of them is missing.	Enter the missing value and click 'Save' again

5.5.41	This is an invalid data value. The new excluded address range is not completely within an IP Address range. Reason: Excluded Address ranges should be completely contained within a single IP Address range specified for the scope. If a DHCP scope contains more than one IP Address range, then the excluded address ranges specified, if any, may not span outside a single IP Address range in any way. This includes overhanging outside of a single IP Address Range or spanning over multiple IP Address Range.	Fix the over-hanging problem. If required, specify multiple excluded address range. Note: As a guideline, use only one IP Address range, and specify multiple excluded ranges to exclude disjoint parts of it.
5.5.45	This is an invalid data value. The new range overlaps with an existing range Reason: This error happens if the specified excluded range overlaps with another excluded address range or with an address that is already assigned to a DHCP Client computer.	Modify the new excluded address range so that it does not overlap with another or does not include assigned IP addresses. You may also go to the client system that go the assigned address and release IP address before setting the excluded range.
5.16.68	This is an invalid operation. You can't delete the last IP Address range in the scope. Reason: The scope contains only one IP Address range and you are attempting to delete it. You must have at least one IP Address range in the scope all the time. You may modify the last entry, however.	Don't delete the last DHCP range. If you need to change it, modify it. If you don't want the DHCP scope to be operational, change its status to 'Disabled'. If don't want any scope operational, set the status of the DHCP Service to 'Disabled'.
8.4.2.	This is an invalid configuration parameter. There was an error in setting data. Reason: You tried to add a port range or filter and the key field didn't contain the characteristic prefix.	If you are adding a new port-range, make sure the 'PortRange (R#)' field is like 'Rxx' where 'xx' is a number. If you are adding a new filter, make sure that 'Filter (F#)' field looks like 'Fxx' where 'xx' is a number.
8.5.3	This is an invalid data value. There was an error in setting port range Reason: You are setting a port range value and the upper and lower limits are not correct or missing.	Each range should begin with a positive even number and must end with a number greater than the beginning number and must be an odd number. Further, the range values should be less than 65535 (64K)
8.8.3	This is an error in data size. There was an error in setting port range. Reason: You are setting a port range that is too big. At present, only 256 ports can be set in the port-range table.	Consult chapter 3 for a discussion on port ranges in QoS. You may not need that big a range. Reduce it to be under 256 ports in the range.

9.4.2	This is an invalid configuration parameter. There was an error in setting data. Reason: This error can happen when you are setting a community string entry, manager entry or a trap community entry. Each entry uses a characteristic key string as its field name. Use 'Cxx' for community strings, 'Mxx' for manager entries and 'Txx' for trap community entries.	Use appropriate key strings in the dialog boxes, as suggested in their labels.
9.6.4 9.6.5 9.6.6	The object was not found. There was an error in setting <object Name> Reason: This error can happen while setting a community string entry, manager address or trap community entry. Each entry takes a characteristic key field as the first field that should follow certain conventions, and a unique number within the class. If that unique number is 0 or less, this error happens.	Specify correct number for the key field name.
10.5.2	This is an invalid data value for requested data. Reason: This can happen happens when user enters values into a dialog box and clicks 'Save' on it. If any of the fields had some strict format specified for it (say dotted format for an IP address) and if you entered a wrong value, it would beep when you tab out of the field. If you ignored that beep, the GUI would reject the field and when you clicked 'Save' it didn't send the field to the Enterprise Edge system, there by causing this problem.	Follow the rules precisely and pay particular attention to 'beeps.' If your IP Address has only 1 digit, prefix them with 0s in order to make them 3-digit in each segments of the dotted notation. If the screen has a scroll bar, scroll and enter all the necessary values.
11.5.2	This is an invalid data value for password. Reason: The user was changing a user profile and the password entered in 'password' and 'confirm password' fields do not match.	Match the passwords.
11.19.9	Failed to Delete. Required at least one user with read-write privilege. Reason: You are attempting to delete the last existing user with READ-WRITE privilege. This operation is not permitted, as it would not allow you to make any other changes to user configuration or other system configuration.	Add another user with read-write privilege before deleting the concerned user id.

11.12.10	Failed to Update. Required at least one user with read-write privilege. Reason: You are attempting to modify the last existing user with READ-WRITE privilege. At this time, no modifications are permitted to the last READ-WRITE user.	Add another user with READ-WRITE privilege before modifying the concerned user id.
14.4.21	Invalid Configuration Parameter. Error in setting interface parameter Reason: You're setting a static route, input filter or output filter under an interface and you didn't enter a correct characteristic key field in the dialog box. Values for these fields should strictly follow the convention provided in the labels for them. It should be something like 'SRxx' for static routes, 'IFxx' for input filters and 'OFxx' for output filters.	Make sure your key names are as per convention and provide unique values for the number component.
14.17.40 14.17.41	Command failed. Error in setting action for input/output filters Reason: You were attempting to set the action for input/output filters on the interface. The operation failed because, there were no input or output filters defined for the interface.	Add an input or output filter before setting the action
14.17.68	Command failed. Error is setting static route. This problem is caused by a mismatch in destination network address in its subnet mask specified in the route.	Match them. Bitwise 'AND' of destination address and subnet mask should be equal to the destination address.
	The routing protocol is changed and the screen didn't update.	Refresh the screen by clicking on 'View Refresh' menu item.
	The routing protocol for the interface shows up as 'RIP'. But no RIP configuration parameters show up on the screen	Set the routing protocol back to 'NONE' and then set to 'RIP' again. The RIP configuration field would show up.
14.5.77	Invalid Data Value. Static default route is not permitted in this version. Reason: You were setting a static route that was a default route for the system. In this release of Enterprise Edge, setting default routes as static routes is not permitted. The default route is managed by the 'Net Link Manager' component that accepts the address of next hop router on the primary and then adds or deletes (manages) the default route in the system.	None

MIB II Information

Here is the mapping between Enterprise Edge counters shown in statistics windows and standard MIB-II variables where applicable.

This section includes:

- Counters shown at LAN and WAN interface levels:
- ICMP Counters
- UDP Counters
- QoS Session Counters
- QoS Best Effort Traffic Counters
- QoS Dropped Packets Counter
- QoS Graph Counters
- QoS Best Effort Queue Counters

Counters Shown at LAN and WAN Interface Levels

1. Byte Received:	ifInOctets
2. Byte Sent:	ifOutOctets
3. Byte Total:	no equivalent (ifInOctets and ifOutOctets)
4. Current Bandwidth:	ifSpeed
5. Output Queue Length:	ifOutQLen
6. Packets Outbound Discarded:	ifOutDiscards
7. Packets Outbound Errors:	ifOutErrors
8. Packets Received Discarded:	ifInDiscards
9. Packets Received Errors:	ifInErrors
10. Packets Received Non-Unicast:	ifInNUcastPkts
11. Packets Received Unicast:	ifInUcastPkts
12. Packets Received Unknown:	ifInUnknownProtos
13. Packets Received:	no equivalent
14. Packets Sent Non-Unicast:	ifOutNUcastPkts
15. Packets Sent Unicast:	ifOutUcastPkts
16. Packets Sent:	no equivalent
17. Packets:	no equivalent

ICMP Counters

Note: Shown under Performance Menu under 'Resources':

1. Messages Outbound Errors:	icmpOutErrors
2. Messages Received Errors:	icmpInErrors
3. Messages Received:	icmpInMsgs
4. Messages Sent:	icmpOutMsgs
5. Messages:	no equivalent (icmpInMsgs + icmpOutMsgs)
6. Received Address Mask:	icmpInAddrMasks
7. Received Address Mask Reply:	icmpInAddrMaskReps
8. Received Destination Unreachable:	icmpInDestUnreachs
9. Received Echo Reply:	icmpInEchoReps
10. Received Echo:	icmpInEchos
11. Received Parameter Problem:	icmpInParmProbs
12. Received Redirect:	icmpInRedirects
13. Received Source Quench:	icmpInSrcQuenchs
14. Received Time Exceeded:	icmpInTimeExcds
15. Received Timestamp Reply:	icmpInTimestampReps
16. Received Timestamp:	icmpInTimestamps
17. Sent Address Mask:	icmpOutAddrMasks
18. Sent Address Mask Reply:	icmpOutAddrMaskReps
19. Sent Destination Unreachable:	icmpOutDestUnreachs
20. Sent Echo Reply:	icmpOutEchoReps
21. Sent Echo:	icmpOutEchos
22. Sent Parameter Problem:	icmpOutParmProbs
23. Sent Redirect:	icmpOutRedirects
24. Sent Source Quench:	icmpOutSrcQuenchs
25. Sent Time Exceeded:	icmpOutTimeExcds
26. Sent Timestamp Reply:	icmpOutTimestampReps
27. Sent Timestamp:	icmpOutTimestamps

UDP Counters

1. Datagrams No Port:	udpNoPorts
2. Datagrams Received Errors:	udpInErrors
3. Datagrams Received:	udpInDatagrams

4. Datagrams Sent:	udpOutDatagrams
5. Datagrams:	no equivalent (udpInDatagrams + udpOutDataGrams)

TCP Counters

1. Connection Failures:	tcpAttemptFails
2. Connections Active:	tcpActiveOpens
3. Connections Established:	tcpCurrEstab
4. Connections Passive:	tcpPassiveOpens
5. Connections Reset:	tcpEstabResets
6. Segments Received:	tcpInSegs
7. Segments Retransmitted:	tcpRetransSegs
8. Segments Sent:	tcpOutSegs
9. Segments:	no equivalent (tcpInSegs + tcpOutSegs)

QoS Session Counters

Note: These are proprietory counters implemented by QoS Provider Module.

1. Not Served Priority Sessions: The number of premium priority sessions declined by the QoS module - probably due to bandwidth restrictions.

2. Requested Priority Sessions: Total number of premium priority sessions requested

3. Served Priority Sessions: Number of premium priority sessions admitted.

QoS Best Effort Traffic Counters

Note: This is a proprietory counter.

1 = Total Best-Effort Octets: Total number octets carried in best-effort level

2 = Total Best-Effort Packets: Total number of packets carried in best-effort level.

QoS Dropped Packets Counter

Note: Proprietory counter in QoS.

1. Total Dropped Octets: Total number of octets dropped, probably due to insufficient buffer.

2. Total Dropped Packets: Total number of dropped packets.

QoS Graph Counters

1. Total Octets: Total number of octets sent by QoS

2. Total Packets: Total number of packets sent by QoS

3. Total Priority Octets: Total number of octets carried in premium priority.

QoS Best Effort Queue Counters

Note: This is a proprietory counter.

1. Total Queue XX Octets: Total number of octets carried at specified queue's priority.

2. Total Queue XX Packets: Total number of packets carried at specified queue's priority.

3. Total Queue XX Packets Dropped: Total number of packets dropped at specified queue - probably due to insufficient buffer space.

Maintenance programming for telephony resources

You can view the Maintenance programming by choosing **Resources**, **Telephony**, **Maintenance**. The Maintenance section of programming has ten headings. For detailed information on maintenance programming, select one of the following.

System version	displays the version number of the system processor.
Module / port status	allows you to check and change the status of modules and ports in your system.
System test log	displays a list of test results, event messages, and alarm codes.
System administration log	displays a list of system initialization sessions, invalid password attempts and password changes.
Network event log	displays a list of events and alarms.
Provisioning	allows you to add or remove individual T1 lines and PRI lines in and out of service.
CSU statistics	displays T1 performance information supplied by the Channel Service Unit.
Tests	allow you to test incoming T1 signals to evaluate transmission quality, the connection between the system and telephones, and the connection between an EE-DTM and the network.
DN-to-port conversion	allows you to determine the port that is associated with a particular DN
Link Status	displays the status of the PRI channel
Debug	used to debug your system

For information on alarm codes and event messages, refer to Alarm codes on page 261 and Event messages on page 261.

System version

System version allows you to check the version of a system. You can use the system version heading to note the version number of the System Processor (SP) software, which resides on the Media Services Card (MSC).

1. Choose **Resources**, **Telephony**, **Maintenance.** The version number of the SP is displayed in the system version box.

2. Write the SP version number on the appropriate Maintenance record.

   The SP version number can be used to determine the software release and the support feature, and to trace any software faults.

Module/port status

Module/port status allows you to view the status of all system modules as well as identify any device or lines connected to the system. This allows you to isolate any malfunctioning part of the system. In addition, you can use **Module/port status** to disable and enable modules and devices. For more information, refer to one of the following procedures.

- Display the module status on page 254
- Disable a module on page 254
- Enable a module on page 255
- Identify a device connected to the system on page 255
- Disable a device on page 256
- Enable a device on page 257

Display the module status

Use this procedure to display module type, the number of sets connected to the module, the number of busy sets and the module's state.

1. Choose **Resources**, **Telephony**, **Maintenance**, **Module/port status.**

   The window displays Modules 01 through to 07. For information on module numbering, refer to Hardware on page 175.

2. Select one of the modules by double-clicking.

   The **Configuration** menu is enabled and the module's status information is displayed.

Disable a module

You must disable a module before you replace it. In addition, you may be able to clear a hung line by disabling and enabling the affected module.

Use Page feature, on your system, prior to disabling.
Use the Page feature to inform people that you are about to disable a module. Indicate that they may experience delays in the performance of their devices.

1. Choose **Resources**, **Telephony**, **Maintenance**, **Module/port status**.

2. Select the module you wish to disable.

   The **State** box indicates that the module is enabled. The **Configuration** menu option is enabled.

3. Select the **Configuration** menu.

   The drop-down menu displays the **Disable** selection.

4. Select **Disable**.

   The system displays a warning that this action will disable the entire module and all of its devices.

5. Click **OK**. The system disables the module in one minute (or immediately, if the status is idle). Press **Cancel** to leave this display without disabling the module.

Enable a module

Use the following procedure to enable a disabled module.

1. Choose **Resources**, **Telephony**, **Maintenance**, **Module/port status**.

2. Select the module you wish to enable.

   The **State** box indicates that the module is disabled and the **Configuration** menu is enabled.

3. Select **Configuration**.

   The drop-down menu displays the **Enable** selection.

4. Select **Enable**.

   The system displays a messaging indicating that the module is being enabled.

Identify a device connected to the system

You may wish to check a device's version number for compatibility with the system. Use the following procedure to display status information for any device connected to the system.

1. Choose **Resources**, **Telephony**, **Maintenance**, **Module/port status**.

   The window displays Modules 01 through to 07. For more information on how modules are numbered, refer to Hardware on page 175.

2. Select one of the modules.

3. Select **Ports on module**.

4. Select one of the ports.

5. Select **Channels**.

6. Select **B1** to display the device connected to the B1 channel or select **B2** to display the device connected to the B2 channel.

   The window displays the device, its type, the version number of the device and it's state.

7. If there is an add-on device attached to the telephone such as a central answering position module or a Busy Lamp Field, select **add on** to display the add-on device.

The following table lists some of the device types that may appear on the Enterprise Edge device identification display.

Display	Explanation
M7100	M7100 telephone
M7310	M7310 telephone
M7324	M7324 telephone
1: CAP1	First CAP module attached to an M7324 telephone
2: CAP2	Second CAP module attached to an M7324 telephone
Nortel Networks ATA 2	Analog Terminal Adapter
BLF	Busy Lamp Field

Disable a device

Give notice that you are disabling equipment.
Inform people that you are going to disable their devices.

Pick a suitable time to disable devices. Disabling a port will disconnect users from their calls.
Do not disable devices when many people are using the Enterprise Edge system. Wait until after regular office hours.

Note: Do **not** enable or disable ports during the first two minutes after plugging your system in. If you do so, incorrect ports may be enabled or disabled. To recover from this, disable, then enable the affected modules using **Module/port status**.

Use the following procedure to disable a device immediately.

1. Identify which device you wish to disable. For information on how to perform this procedure, refer to Identify a device connected to the system on page 255.

2. Select **Disable**. The system displays a warning that this action will disable the port.

3. Select **OK**. The system disables the device in one minute (or immediately, if the device is idle). Press **Cancel** to leave this display without disabling the device.

Enable a device

Use the following procedure to enable a disabled device:

1. Identify which device you wish to disable. For information on how to perform this procedure, refer to Identify a device connected to the system on page 255.

2. Select the device and then select **Enable**.

   The system displays a messaging indicating that the device is being enabled.

System test log

The System test log shows you a list of diagnostic test results, audits, event messages, and alarm codes. By using this feature you can check log items, any current alarms, timing of log events and the number of consecutive occurrences of an event or an alarm. In addition, you can use the **System test log** selection to erase the log.

The System test log holds a maximum of 20 items. You should check and record these items at regular intervals. Erase the log after dealing with all the items.

Use the **System test log** selection under **Maintenance** to perform one of the following procedures.

- Display information on the items in the System test log on page 257
- Erase the log on page 258

Display information on the items in the System test log

You can display information on any item in the System administration log using the following procedure.

1. Choose **Resources**, **Telephony**, **Maintenance**, **System test log.**

2. If the Unified Manager indicates that there are hidden subheadings, double click on the heading to display all the items in the log. If there are no log entries, the Unified Manager will indicate that there are no hidden subheadings.

3. Select any item. Information about the log item is displayed.

   The description attribute indicates if the item is an event or alarm and includes the associated code. The time the event or alarm occurred is displayed. For more information on the event or alarm, refer to Alarm codes on page 261 or Event messages on page 261.

   Note: Alarms are also displayed in the Windows NT event log.

4. Write down the item on the System administration log record and repeat these steps until you have recorded all the items.

Erase the log

You can erase the displayed log items from the System Test log using the following procedure.

Note: You cannot remove selected log items. You only have the option of removing all the log items.

1. Choose **Resources**, **Telephony**, **Maintenance**, **System test log.**

2. If the Unified Manager indicates that there are hidden subheadings, double click on the heading to display all the items in the log. If there are no log entries, the Unified Manager will indicate that there are no hidden subheadings.

3. Select the **Del All** button from above the left hand window.

   The system displays a message asking you to confirm that you wish to remove all of the items.

4. Select **Yes** to continue. If new items have been added since the log items were displayed, these new items are not erased.

System administration log

The System administration log keeps a record of administrative events such as sessions in which a change was made, invalid password attempts, and password changes. By using this feature you can check the items in the log, check when each item in the log occurred and you can erase the log.

The System administration log holds a maximum of ten items. Erase the log after dealing with all the items.

Use the **System admin log** selection under **Maintenance** to perform one of the following procedures.

- Display information on the items in the System Administration log on page 259
- Erase the log on page 259

Display information on the items in the System Administration log

You can display information on any item in the System administration log using the following procedure.

1. Choose **Resources**, **Telephony**, **Maintenance**, **System admin log.**

2. If the Unified Manager indicates that there are hidden subheadings, double click on the heading to display all the items in the log. If there are no log entries, the Unified Manager will indicate that there are no hidden subheadings.

3. Select any item. Information about the log item is displayed.

   The description attribute indicates if the item is an event or alarm and includes the associated code. The time the event or alarm occurred is displayed. For more information on the event or alarm, refer to Alarm codes on page 261 or Event messages on page 261.

   Note: Alarms are also displayed in the Windows NT event log.

4. Write down the item on the System administration log record and repeat these steps until you have recorded all the items.

Erase the log

You can erase the displayed log items from the System Administration log using the following procedure.

Note: You cannot remove selected log items. You only have the option of removing all the log items.

1. Choose **Resources**, **Telephony**, **Maintenance**, **System admin log.**

2. If the Unified Manager indicates that there are hidden subheadings, double click on the heading to display all the items in the log. If there are no log entries, the Unified Manager will indicate that there are no hidden subheadings.

3. Select the **Del All** button from above the left hand window.

   The system displays a message indicating that this will remove all of the items.

4. Select **Yes** to continue. If new items have been added since the log items were displayed, these new items are not erased.

Network event log

The Network event log keeps a record of events and alarms that are specific to the T1 network interface. By using this feature you can check the items in the log, check when each item in the log occurred and you can erase the log.

The Network event log holds a maximum of twenty items. Erase the log after dealing with all the items.

Use the **Network event log** selection under **Maintenance** to perform one of the following procedures.

- Displaying information on the items in the Network event log on page 260
- Erase the log on page 260

Displaying information on the items in the Network event log

You can display information on any item in the Network event log using the following procedure.

1. Choose **Resources**, **Telephony**, **Maintenance**, **Network event log**.

2. If the Unified Manager indicates that there are hidden subheadings, double click on the heading to display all the items in the log. If there are no log entries, the Unified Manager will indicate that there are no hidden subheadings.

3. Select any item. Information about the log item is displayed.

   The description attribute indicates if the item is an event or alarm and includes the associated code. The time the event or alarm occurred is displayed. For more information on the event or alarm, refer to Alarm codes on page 261 or Event messages on page 261.

   Note: Alarms are also displayed in the Windows NT event log.

4. Write down the item on the System administration log record and repeat these steps until you have recorded all the items.

Erase the log

Note: You cannot remove selected log items. You only have the option of removing all the log items.

1. Choose **Resources**, **Telephony**, **Maintenance**, **Network event log.**

2. If the Unified Manager indicates that there are hidden subheadings, double click on the heading to display all the items in the log. If there are no log entries, the Unified Manager will indicate that there are no hidden subheadings.

3. Select the **Del All** button from above the left hand window.

   The system displays a message indicating that this will remove all of the items.

4. Select **Yes** to continue. If new items have been added since the log items were displayed, these new items are not erased.

Alarm codes

The Enterprise Edge system generates alarm codes after system disconnections or after certain anomalies in system operation. All alarm codes appear at the Alarm telephone, in the System test log of a Maintenance session and in the Win NT event log. For a more complete description of alarm and event codes consult your technical support representative.

Tips - The Alarm telephone is assigned in Feature settings under System programming.

Alarms have a higher severity than events. Attend to alarm codes before event messages.

Alarm code information that is specific to Companion components is included in the Companion event messages on page 266

An alarm code may not be displayed until two minutes after it has been triggered. If the system is powered off when the alarm is triggered, the alarm code is not displayed until two minutes after the system is powered on.

Event messages

Event messages appear as items in the System administration log or the System test log of the Maintenance session. Most of these event messages can only be caused by an unusual combination of events, and should rarely occur.

Each event is assigned a severity number. An “S” preceding this number, “S4” for example, may appear in the event message. “S9” is the most severe. If the log is full, new event messages with a higher severity number replace existing event messages of a lower severity. For this reason, you should check event messages at regular intervals. You can then deal with all messages before they are replaced. The time that the message is recorded is also provided.

Event message information that is specific to Companion components is included in the Companion event messages on page 266.

For every event message that you see:

1. Refer to Significant event messages on page 262.

2. Determine if the event caused the system to automatically restart. For more information, refer to the table on Event Message on page 264.

Significant event messages

The following table lists event messages that are relevant to maintenance activities.

Event message	The event message is recorded when…
Evt:210-YYYZ S4	Loopback test YYY on Trunk module Z has been started
Evt:211-YYYZ S4	Loopback test YYY on Trunk module Z has been stopped
Evt:220-3546 S4	the Sys admin log has been cleared by the DN (3546 in this case)
Evt:221-3546 S4	the Sys test log has been cleared by the DN (3546 in this case)
Evt:222-3546 S5	the DN (3546 in this case) enters the debugging facility that is password protected
Evt:255 S9	administered mode is not supported by the module plugged into the slot
Evt:260-0302 S8	the system takes the access line on port 0302 out of service because no current was detected
Evt:261-0302 S1	the access line on port 0302 is returned to service after current was detected (see Evt:260)
Evt:268-07 S8	Dialing filter 07 has lost data due to a fault in the system memory
Evt:269-3546 S8	the Line/set filter for the DN (3546 in this case) has lost data due to a fault in the system memory
Evt:299 S1	the system powers up after a power failure
Evt:327 S5	short term alarm threshold has been surpassed in the EE-DTM
Evt:328 S5	short term alarm threshold has been surpassed in the EE-DTM
Evt:329 S5	short term alarm threshold has been surpassed in the EE-DTM
Evt:330 S5	short term alarm threshold has been surpassed in the EE-DTM
Evt:336 S5	long term alarm has been surpassed in the EE-DTM
Evt:373 S5	the system restart diagnostic tool has been activated
Evt:407 S2	there are no more codes for Speed Dial numbers
Evt:408 S2	there is no more memory for Speed Dial codes
Evt:415-3546 S3	an invalid customer password has been entered by the DN (3546 in this case)
Evt:418 S7	a DN change is successful
Evt:419 S2	the time setting has been changed
Evt:421 S8	a DN change failed
Evt:422-3546 S6	a length change by the DN (3546 in this case) has been requested
Evt:423-3546 S6	an individual DN change has been requested by the DN (3546 in this case)
Evt:441 S2	a timeout occurred while waiting for ANI or DNIS digits to be received

Event message		The event message is recorded when…
Evt:442	S5	a timeout occurred while waiting for ANI or DNIS digits to be received
Evt:454	S5	Invalid password entered
Evt:458	S4	Call-by-Call NVRAM data is corrupt and all the values have been reset to default.
Evt:459	S9	DN length has been changed to less than 3 digits
Evt:680	S9	wireless system is disabled
Evt:681	S9	activation or recovery code entered
Evt:683	S9	new base station configuration detected
Evt:687	S4	the data driver has received a bad call reference
Evt:688	S4	the data driver has received a bad data event
Evt:689	S4	the data driver could not allocate a new index
Evt:690	S4	no response to the system within 10 seconds of being sent an initialization message
Evt:691	S4	no response to the system within 3 seconds
Evt:692	S4	a bad parameter value has been received in a stimulus message from the data device
Evt:693	S3	old data to be discarded has been detected
Evt:694	S4	RADAR flow control has received a bad stimulus message from an off-core application
Evt:695	S4	attached set denied request for a B-channel
Evt:696	S2	corrupt CLID length
Evt:697	S2	an asynchronous data report generated by SDI
Evt:698	S8	incorrect software key entered
Evt:799	S7	a call processing error has occurred on an ISDN line
Evt:822	S8	Alarm code 63 is sent because there are no DTMF receivers for an incoming call
Evt:882	S9	mobility data re-evaluation sequence initiated
Evt:883	S4	an invalid dial pulse signal was received by the EE-DTM
Evt:992	S6	auto attendant error

How to read an event message

In the event message shown below, Evt799 indicates a call processing error has occurred on an ISDN line.

Evt799-XXXX YYS7

The event number Evt799 is followed by a number representing the line or loop number, and a code for the type of error. In this example, the error has occurred on line XXX and the error code is YY.

The following table lists the error codes and their meanings.

Error code	Meaning
01	Internal software error. Cannot acquire the B-channel from the B-channel arbitrator.
02	Internal software error. There is no free line available for the call.
03	A call that is not on the B-channel has been attempted. These kind of calls are part of EKTS service, which is not supported by this version of the software. Check with your service provider to make sure your package does not include EKTS service.
04	Internal software error. Failed to instantiate on the chain.
05	Internal software error. Activation procedure failed.
06	Internal software error. Index conversion failed.
07	Unexpected digits on a Manual answer mode line. Configuration of the system and the network connection may not match.
09	Cannot get vterm (virtual terminal) from the Vterm Server.
0C	Internal software error. Already instantiated on the chain.

Events that cause a system restart

You should rarely see any event messages that are not described in the Significant event messages on page 262. If you do see one of these event messages, the system has followed its normal recovery from an unusual combination of system events. Although the problem is not a serious one, repeated occurrences of the event number should be reported as soon as possible.

As a result of some events, the system automatically restarts itself. The table on the next two pages lists all the event numbers and identifies which of these events are associated with system restarts.

Most of these events are recorded in the **System test log**. The few exceptions to this are recorded in the **System administration log**, as indicated.

Event Message	System Restart	Event Message	System Restart
101-106	Yes	400 (Admin log)	Yes
107	No	401-403	No
108-112	Yes	405-411	No
113	No	412-419 (Admin log)	No
114-116	Yes	421-423 (Admin log)	No
117	No	424-425	No
118-120	Yes	426-430	Yes
121-123	No	431	No
124-125	Yes	432	Yes
126-129	No	433	No
130	Yes	441-442	No
131-132	No	453	No

Event Message	System Restart	Event Message	System Restart
133-134	Yes	454	No
135-136	No	458-459	No
137	Yes	600-602	Yes
138-150	No	603-613	No
151	Yes	614	Yes
152	No	615-629	No
160-164	No	630	Yes
170-173	No	631-646	No
200-211	No	680	No
220 (Admin log)	No	681	No
221-222	No	683	No
223 (Admin log)	No	689-698	No
224	Yes	799	No
225-228	No	800-802	No
229 (Admin log)	No	803	Yes
230-235	No	804-807	No
245-248	Yes	808	Yes
250-256	No	809	No
260-271	Yes	810	Yes
280-283	No	811-820	No
285-298	Yes	823	Yes
299	No	824-825	No
327	No	851	No
328	No	882	No
329	No	883	No
330	No	900	No
336	No	940-943	No
373	No	950-989	No

Companion event messages

Table 1 Event messages

Event message display	Cause
Evt:275-3546 S8	(U.S. only) Unable to activate all registered portables. The system ran out of portable credits. One event is generated per portable that failed to activate. The repetition of the corresponding alarm code 59 indicates how many additional credits must be purchased.
Evt:301-1031 S5	The Base Station (on port 0103 in this case) cannot successfully receive the data image. Both radios belonging to the Base Station are disabled. This may occur if the flash EEPROM is faulty. Two events are raised: one for the B1 channel radio (as in this case) and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:302-1031 S5	The Base Station (on port 0103 in this case) cannot be written to during data transfer. Both radios belonging to the Base Station are disabled. The Base Station's flash EEPROM is faulty. Two events are raised: one for the B1 channel radio (as in this case) and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:303-1031 5	The Base Station (on port 0103 in this case) cannot be synchronized with the other Base Stations in the system. Both radios belonging to the Base Station are disabled. The Base Station hardware is faulty. Two events are raised: one for the B1 channel radio (as in this case) and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:304-1032	A B2 channel radio (radio 2 on port 0103 in this case) cannot be synchronized with other radios because of system overload.
Evt:305-01032 S5	A B2 channel radio (radio 2 on port 0103 in this case) cannot be synchronized because the B1 radio was disabled in maintenance. Both radios belonging to the Base Station (on port 0103 in this case) are disabled. The B1 radio must be operational to synchronize both radios of the Base Station with other radios in the system. Two events are raised: one for the B1 channel radio and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:306-01031 S5	A radio (0103-1 in this case) cannot be synchronized because there are no B2 channel radios. Both radios belonging to the Base Station (on port 0103 in this case) are disabled.Two events are raised: one for the B1 channel radio in this case) and another for the B2 channel radio. A corresponding alarm code 53 occurs.
Evt:307-0109100 S5	A recoverable RIM fault has occurred The RIM is reset. If a link is active when this error occurs, the link is dropped. The radio (0109-1 in this case) is returned to service.

Event message display	Cause
Evt:307-0109101 S5	An unrecoverable RIM fault has occurred The radio (0109-1 in this case) is disabled and taken out of service. If a link is active when this error occurs, the link is dropped. A corresponding alarm code 53 occurs.
Evt:307-0109102 S5	The built-in self-test on the Base Station has failed The radio (0109-1 in this case) is disabled and taken out of service. If a link is active when this error occurs, the link is dropped. A corresponding alarm code 53 occurs.
Evt:308-0103 S5	The Base Station is connected to a system that supports a radio protocol that the Enterprise Edge does not understand.
Evt:664 S8	There is a bad signature.
Evt:665 S4	(U.S. only) there are insufficient radio credits.
Evt:666 S5	(U.S. only) radio credits decreased.
Evt:667 S5	(U.S. only) UTAM keys are required.
Evt:668 S5	(U.S. only) UTAM test failed.
Evt:669 S5	Evaluation override is finished.
Evt:670 S5	Disablement test is active.
Evt:671 S5	Disablement test is finished.
Evt:672 S5	System initialization is beginning.
Evt:673 S5	System initialization is finished.

Event message display	Cause
Evt:675 S5	Demo system.
Evt:831 S5	Software error dealing with Base Station.
Evt:832 S5	System problem with locating portable telephones.
Evt:833 S5	The radio driver software which directly controls the Base Stations' device has experienced an internal error.
Evt:834 S5	System problem with locating portable telephones.
Evt:835 S5	Wireless system access error.
Evt:836 S5	Wireless system access error.
Evt:837 S5	Trying to register an incompatible wireless device.
Evt:840 S5	Wireless system software error in dealing with a portable telephone.
Evt:841 S5	Wireless system software error.
Evt:842 S5	Portable does not support specific display character.
Evt:843 S5	Internal radio driver error.
Evt:848 S5	A cell manager has been unable to register with the router.

Event message display	Cause
Evt:849 S5	Synchronization error.
Evt:850 S5	Synchronization error.
Evt:851 S5	Base Station software error.
Evt:852 S5	The Data Transfer server has been told by the Base Station that an error has occurred.
Evt:853 S5	The Data Transfer server has been told by the Base Station that an error has occurred.
Evt:854 S5	Invalid event for Data Transfer.
Evt:855 S5	Internal wireless subsystem software error.
Evt:856 S5	Internal wireless subsystem locator error.
Evt:859 S5	All possible wireless telephone numbers have been registered to portable telephones. No directory number is available to handle the registration Link setup request.
Evt:864 S5	A Base Station has received a corrupted stimulus message.
Evt:865 S5	The Base Station does not understand the received stimulus message. This occurs when you are trying to use a type of portable that the system does not support.
Evt:869 S5	Wireless subsystem language loading error.
Evt:870 S5	Firmware downloading to Base Station.

Event message display	Cause
Evt:871 S5	Basestation download is complete.
Evt:872 S5	Wireless subsystem error.
Evt:873 S5	Wireless subsystem Common Signaling Channel server software error.
Evt:877 S5	Wireless auto-admin (Re-Eval) subsystem detected that a data re-evaluation is required.
Evt:878 S5	Wireless data re-evaluation has started.
Evt:879 S5	Wireless data re-evaluation has completed.
Evt:881 S5	Wireless auto-admin (Re-Eval) indicating that a configured cell failed to come on-line. Alarm 23 displays cell that failed.
Evt:884 S5	The Wireless auto-admin (Re-Eval) subsystem has detected an error.
Evt:885 S5	Sequencer functionality has detected an error.
Evt:886 S5	The Wireless auto-admin (Re-Eval) Initial Intelligence component has detected an error.
Evt:887 S5	The Wireless auto-admin (Re-Eval) radio Sniffing component has detected an error.
Evt:888 S5	The Wireless auto-admin (Re-Eval) Radio Manager has detected an error.

Note: Companion alarm codes are displayed in the Windows NT™ event log.

Provisioning

Use the **Provisioning** selection under **Maintenance** to perform one of the following procedures.

- Provision a T1 line on page 271
- Provision a PRI line on page 271
- Deprovision a line on page 271
- Disable a PRI Channel on page 272

Provision a T1 line

1. Choose **Resources**, **Telephony**, **Provisioning.**
2. Select a module.
3. Select the appropriate card. The display shows the card type.
4. Select **Provision lines**. All the available lines are displayed.
5. Select one of the lines. If the line has not been provisioned, the status box displays **Deprovisioned**.
6. Select **Provisioned** from the drop-down menu.

Provision a PRI line

ISDN lines are provisioned by default. For more information on adding a EE-DTM (configured as PRI) see Modules under Hardware.

Deprovision a line

Deprovisioning all of the lines on an EE-DTM does not disable the module.

1. Choose **Resources**, **Telephony**, **Provisioning**.
2. Select a module.
3. Select the appropriate card. The display shows the card type.
4. Select **Provision lines**. All the available lines are displayed.
5. Select one of the lines. If the line has been provisioned, the status box displays **Provisioned**.
6. Select **Deprovisioned** from the drop-down menu.

Disable a PRI Channel

PRI channels can be disabled however, there is no association between a line number and a b-channel. Disabling of a b-channel can be done when you have fractional PRI. For more information, refer to Link Status on page 278.

Tests

Enterprise Edge allows you to run tests which verify the integrity of the installation wiring for the telephone sets. Before you run any tests, use the procedure, DN-to-port conversion on page 274, to determine the port that is associated with a particular DN.

Choose an appropriate time to run tests.
A good time to run tests is after office hours.

The following messages may appear on the Alarm Telephone during Loopback tests.

Message	Explanation
EVT: 210-YYYZ	Loopback test YYY on Trunk module Z has started
EVT: 211-YYYZ	Loopback test YYY on Trunk module Z has ended

Loopback tests are started and stopped in **Maintenance** programming under the heading **Tests**. Only one test at a time can be run on an EE-DTM. You can exit **Maintenance**, or move on to another programming task while the loopback test is running. While the loopback test is running, the green “in Service” LED on the EE-DTM flashes.

If the internal CSU is administered on a line loopback and payload loopback, tests can also be invoked and stopped by the central office. In order to be able to run a payload loopback test, the EE-DTM must be configured for extended superframe format.

The Enterprise Edge system allows you to run the following tests:

- Line loopback test on page 273
- Payload loopback test on page 273
- Card loopback test on page 273
- Continuity loopback test on page 273

Use the procedure, Start a loopback test on page 273, to run any of these tests.

Line loopback test

The line loopback test loops the full 1.544 Mbps signal received from the network back to the network. The looped signal is regenerated without any change in the framing format and without the removal of any bipolar violations. The line loopback test can also be invoked and stopped remotely using the in-band signal or via the facility data link (FDL) in extended super frame (ESF) format.

The line loopback test must be run in coordination with the T1 or PRI service provider. Some test patterns can cause the EE-DTM to reset. To avoid this, start the line loopback test from your system before the T1 or PRI service provider begins their test, and stop the line loopback test from your system after the T1 or PRI service provider ends their test.

Payload loopback test

The payload loopback test loops the received information bits (192 per frame) back to the network. The payload loopback test can also be invoked and stopped remotely via the facility data link (FDL) in extended super frame (ESF) format.

The payload loopback test must be run in coordination with the T1 service provider. Some test patterns can cause the EE-DTM to reset. To avoid this, start the payload loopback test from your system before the T1 service provider begins their test, and stop the payload loopback test from your system after the T1 service provider ends their test.

Card loopback test

The card edge loopback test loops the outgoing signal on the EE-DTM back to its internal received signal path. Signal paths to the external network are disconnected.

Continuity loopback test

The continuity loopback test shorts the tip and ring pair of the receive signal path with the transmit signal path. This test allows you to check the metallic continuity of the external wiring.

Start a loopback test

Give notice that you are running a loopback test.
Calls on all T1 or PRI lines on the EE-DTM will be automatically dropped when a loopback test is invoked. Use the Page feature to notify people using the system that a test is about to begin and that calls will be disconnected.

1. Choose **Resources**, **Telephony**, **Maintenance**, **Tests**.

2. Select the module which contains the card you want to test.

3. Select the appropriate card.

   The **Configuration** menu option is enabled. The loopback status box displays the type of test currently running.

   Note: If there is an analog module in the slot or the slot is empty, the box displays **Not equipped**.

4. From the **Configuration** menu option, select **Start loopback** to begin the test.

   The system displays the Loopback type selection window.

5. From the drop-down menu, select the test you want to run and then select **OK**.

   The options are **line**, **payload**, **card edge** or **continuity**. After you select the test, the test name is displayed.

   Note: You may end the test at any time by selecting **Stop loopback** from the **Configuration** menu option.

DN-to-port conversion

If you know a telephone's DN, you can determine the port that is associated with this DN, using the following procedure.

1. Choose **Resources**, **Telephony**, **Maintenance**, **DN-to-Port Conversion**.

   The window displays a number of fields.

2. Type the DN in the **DN to convert** box and press **Enter**.

   The system displays values in the Device port and Device channel fields.

CSU statistics

Each EE-DTM is equipped with an internal channel service unit (CSU). When enabled, the internal CSU monitors the quality of the received T1 signal and provides performance statistics, alarm statistics and diagnostic information.

EE-DTMs must be individually programmed to establish parameters for collecting and measuring transmission performance statistics by the CSU.

For more information, refer to:

- Statistics collected by the Enterprise Edge system on page 275
- Enable the internal CSU on page 275
- Check the performance statistics on page 276
- Check the CSU alarms on page 276
- Check carrier failure alarms on page 277

- Check bipolar violations on page 277
- Check short term alarms on page 277
- Check Defects on page 277
- Reset all statistics on page 278

Statistics collected by the Enterprise Edge system

Three performance parameters are accumulated:

- errored seconds (ES)
- severely errored seconds (SES)
- unavailable seconds (UAS)

These parameters are defined as per TIA-547A. Errored seconds are enhanced to include control slip (CS) events. Only near-end performance data is recorded.

The internal CSU continuously monitors the received signal and detects four types of transmission defects:

- any active carrier failure alarms (CFA) (loss of signal LOS, out of frame OOF, alarm indication signal AIS, remote alarm indication RAI)
- the number of bipolar violations that occurred in the last minute
- any defects (loss of signal LOS, out of frame OOF, alarm indication signal AIS) that occurred in the last minute
- the number of milliseconds of short term alarms (loss of signal LOS, out of frame OOF, alarm indication signal AIS, remote alarm indication RAI) in the last minute. A short term alarm is declared when the detected defects persist for tens of milliseconds.

A carrier failure alarm (CFA) is a duration of carrier system outage. CFA types reported can be mapped to CFAs defined in TIA-547A and TR62411 as follows:

Enterprise Edge	TIA-547A	TR62411
LOS CFA	Red CFA	Red CFA
OOF CFA	Red CFA	Red CFA
AIS CFA	Red CFA	AIS CFA
RAI CFA	Yellow CFA	Yellow CFA

The criteria for declaring and clearing the alarms is selectable to meet those in TIA-547A or TR64211.

Enable the internal CSU

Use the following procedure to enable the internal CSU to gather performance statistics for your T1 lines or PRI with public interface.

1. Choose **Resources**, **Telephony**, **Hardware**, and select the appropriate module.

2. Select a card.

3. Select **T1 parameters**.

4. In the **Internal CSU** box, select **On** from the drop-down menu.

   The card will be temporarily disabled while the internal CSU is being enabled.

Check the performance statistics

1. Choose **Resources**, **Telephony**, **Maintenance**, **CSU statistics**.

2. Select a module.

3. Double click on one of the cards.

   The screen displays the card statistics, including the date and time that the system began collecting statistics.

4. Select **Performance statistics** to view the performance statistics.

5. Select **Current interval** to display the duration of the current 15 minute interval of the selected card, the number of errored seconds (ES), the number of severely errored seconds (SES) and the number of unavailable time seconds (UAS).

6. Select **15 min intervals** to display statistics for 15 minute intervals in the last 24 hours, numbered from the most recent (01) to the oldest (96). Enter an interval number, or select the most recent interval. The display shows the start time of the interval.

7. Select **24 hour summary** for an overall summary of the previous 24 hours. The number of intervals are displayed in the summary.

Check the CSU alarms

1. Choose **Resources**, **Telephony**, **Maintenance**, **CSU statistics**.

2. Select a module and then select a card.

3. Select **Alarm statistics** and then select **Active alarms**.

   The display shows all the active alarms of the types **LOS (loss of signal)**, **OOF** (out of Frame), **RAI** (Remote alarm indicator) or **AIS** (Alarm indication signal). For more information on these types of transmission defects, refer to Statistics collected by the Enterprise Edge system on page 275.

Check carrier failure alarms

1. Choose **Maintenance**, **CSU statistics.**
2. Select a module and then select a card.
3. Select **Alarm statistics**.
4. Select **CFA alarms**.

   The display shows **LOS (loss of signal)**, **OOF** (out of Frame), **RAI** (Remote alarm indicator) or **AIS** (Alarm indication signal). For more information on these types of transmission defects, refer to Statistics collected by the Enterprise Edge system on page 275.
5. Select the type of alarms you wish to view.

   The display shows the alarms and the periods for which alarms have been collected.

Check bipolar violations

1. Choose **Resources**, **Telephony**, **Maintenance**, **CSU statistics**.
2. Select a module and then select a card.
3. Select **Alarm statistics** by double clicking.

   The display shows the number of bipolar violations that occurred in the last minute.

Check short term alarms

1. Choose **Resources**, **Telephony**, **Maintenance**, **CSU statistics**.
2. Select a module and then select a card.
3. Select **Alarm statistics.**
4. Select **ShortTerm alarms**.

   The display shows the short term alarms and the number of milliseconds (not necessarily contiguous) that were active in the last minute.

Check Defects

1. Choose **Resources**, **Telephony**, **Maintenance**, **CSU statistics**.

2. Select a module and then select a card.

3. Select **Alarm statistics** and then select **Defects**.

   The display shows the first type of defect and the number of milliseconds (not necessarily contiguous) the hardware reported it active in the last minute.

Reset all statistics

1. Choose **Resources**, **Telephony**, **Maintenance**, **CSU statistics**.

2. Select a module and then select a card.

3. From the **Configuration** menu, select **Clear CSU statistics.**

   The system displays a message indicating that this will remove all of the statistics.

4. Select **OK** to erase all the current statistics and begin collecting statistics again.

Link Status

When you purchase PRI from your service provider, you can request the number of B-channels that are allocated for you to use. For example, you may want to use only 12 B-channels instead of 23 B-channels. If this is your situation, you should disable all the B-channels that you do not need.

It is recommended that the number of lines that are deprovisioned on an EE-DTM (configured as PRI) be the same as the number of b-channels that are disabled. For example, If the EE-DTM is on bus 7, when b-channels 13-23 are disabled, you should deprovision lines 73 to 83.

Start with the display showing **Maintenance**

1. Choose **Resources**, **Telephony**, **Maintenance**, **Link status**.

2. Select the module and card

3. Select **B channels**.

   A list of the B channels on this card is displayed.

4. Select a channel

   The display shows the status of the PRI channel.

5. In the **Configuration** menu, select **Enable** or **Disable** to change the setting for the channel.

Metrics

The following usage metrics are available with the Enterprise Edge Software:

- Hunt group metrics on page 279
- Call-by-Call on page 279

Hunt group metrics

This feature gives you statistical information on hunt group calls.

1. Choose **Resources**, **Telephony**, **Metrics**, **Hunt Group Metrics**.

   The hunt groups are displayed up to a maximum of 30.

2. Select the group number.

   The display shows all the statistical information for the selected hunt group.

To clear the hunt group metrics, **Clear group** under the **Configuration** menu.

Call-by-Call

This feature gives you statistical information on call-by-call limit settings for PRI when the protocol is set to call-by-call routing.

1. Choose **Resources**, **Telephony**, **Metrics**, **CbC limit metrics**.

   The display shows the pools that supports CbC routing.

2. Select a pool

   The display shows the services in the pool. The services that are displayed depends upon the PRI protocol.

3. Select a service.

   The display shows the settings for the selected service.

To clear the settings for a selected service, select **Clear metrics** under the **Configuration** menu.

Moving telephones

You can move a Enterprise Edge telephone to a new location within the system without losing its programmed settings. Set relocation (automatic telephone relocation) must be enabled in system programming. This makes the internal numbers, autodial settings, and personal speed dial codes remain with the telephone when it is unplugged.

Automatic telephone relocation is disabled by default. Use the following procedure to enable set relocation.

1. Choose **Resources**, **Telephony**, **General settings**, **Feature settings**.

2. In the Set relocation box, select **Y** from the pull-down menu.

After set relocation is enabled, unplug the telephone and plug it in again at another location. It may take up to 45 seconds for the system to recognize the telephone.

Tips - All telephones being moved should be relocated before new telephones are plugged into their place. This allows the moved telephones to retain their programmed settings. If a new telephone is plugged into the system before the old telephone is reconnected at a new location, the system will give the old telephone's information to the new telephone, and the old telephone will no longer be recognized by the system.

When changing a telephone's internal number (in programming), wait one minute after Automatic Telephone Relocation.

When you relocate a telephone, the telephone must remain installed and connected in the new location for at least 3 minutes for the programming relocation to be complete. Moving the telephone again before the 3 minute period may result in losing the telephone's programming.

Troubleshooting your Enterprise Edge system

10

These troubleshooting procedures allow you to solve many problems in the Enterprise Edge system. Follow these procedures before replacing any components.

Only qualified persons should service the system.
The installation and service of this unit is to be performed only by service personnel having appropriate training and experience necessary to be aware of hazards to which they are exposed in performing a task and of measures to minimize the danger to themselves or other persons.

Electrical shock hazards from the telecommunication network and AC mains are possible with this equipment. To minimize risk to service personnel and users, the Enterprise Edge must be connected to an outlet with a third-wire ground.

Service personnel must be alert to the possibility of high leakage currents becoming available on metal system surfaces during power line fault events near network lines. These leakage currents normally safely flow to Protective Earth ground via the power cord. Therefore, it is mandatory that connection to an earthed outlet is performed first and removed last when cabling to the unit. Specifically, operations requiring the unit to be powered down must have the network connections (central office lines) removed first.

For more information, refer to the following sections.

- General troubleshooting information on page 281
- Problems with telephones on page 284
- Problems with lines on page 285
- Problems with optional equipment on page 291
- Problems with Trunk or Station Modules on page 295
- Problems for network or remote users on page 296
- Problems with Companion sets on page 302

General troubleshooting information

- Getting ready on page 281
- Types of problems on page 282
- Basic troubleshooting procedure on page 282

Getting ready

Before you begin troubleshooting, gather all the information that is relevant to your network configuration such as:

- records from people who use the network
- information about other hardware and non-Enterprise Edge features within the public or private network

> ***Notify service provider of T1 or PRI signaling disruption.***
> Notify your T1 or PRI service provider before disconnecting your T1 or PRI lines, removing power to your system, or performing any other action that disrupts your T1 or PRI signaling. Failure to notify your T1 or PRI service provider may result in a loss of T1or PRI service.

Types of problems

The problems you encounter will likely fall into one of the following categories:

Misunderstanding of a feature: A problem may be reported because an Enterprise Edge user is unfamiliar with the operation of a given feature. You may be able to solve the problem simply by demonstrating how to use the feature correctly.

Programming errors: You may encounter problems caused by errors in programming. A feature may have been programmed incorrectly or may not have been programmed at all.

Wiring connections: Wiring problems are caused by loose, unconnected, or incorrect wiring. Use the procedures in the section on checking the hardware as a guide.

Equipment defects: You may encounter problems caused by Enterprise Edge equipment defects. See the appropriate section for problems related to the system hardware.

Basic troubleshooting procedure

Use the following basic troubleshooting procedure as well as the detailed descriptions in this guide. Where more than one procedure is given for a particular problem, the procedures represent different options from which you should select just one.

1. Diagnose the trouble by determining:
   - the types of problems users have experienced
   - the frequency of the problems
   - how many telephones are affected
2. Access the system performance graphs and tables to view the system usage and any system faults. For more information, refer to Viewing system performance and fault alarms on page 283.

3. Check how a feature is being used. A problem may have been reported because of a misunderstanding about how a feature works. Confirm that the person who reported a problem understands the intended use and operation of any feature in question.

4. Run a Station set test (Feature 8 0 5).

5. Check the wiring and hardware connections.

6. If the problem persists, run a Maintenance session as described in Maintenance programming for telephony resources on page 253.

7. If hardware is defective, replace it. If the trouble requires expert advice, use the instructions in How to Get Help on page 283.

How to Get Help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone Number
Billerica, MA	800-2LANWAN (800-252-6926)
Santa Clara, CA	800-2LANWAN (800-252-6926)
Valbonne, France	33-4-92-96-69-68
Sydney, Australia	61-2-9927-8800
Tokyo, Japan	81-3-5402-7041

Viewing system performance and fault alarms

- System performance graphs and tables on page 283
- System Fault Alarm Banner on page 284

System performance graphs and tables

To access the system performance graphs and tables:

1. Choose **Performance** and then click **System CPU Usage Graph**.
The System CPU Usage Graph appears.

2. Choose **Performance** and then click **System CPU Usage Table**.
The System CPU Usage Table appears.

3. Access the Memory Usage graph and Memory Usage table by following the steps for System CPU Usable Graphs and Tables.

For information on using performance tables and graphs, refer to Graphs and tables on page 243.

System Fault Alarm Banner

To access the system fault alarm banner:

1. Choose **Configuration** and then click **Fault**.
   The Alarm Banner dialog box appears.

Problems with telephones

For troubleshooting information for your telephone sets, refer to one of the following items:

- Telephone has faulty buttons, display, handset or other hardware problems on page 284
- Digital telephone display unreadable on page 284
- Telephone dead on page 285

Telephone has faulty buttons, display, handset or other hardware problems

Run a Station Set Test (Feature 8 0 5).

Digital telephone display unreadable

If the trouble is with an M7310 or an M7324 telephone

1. Press Feature * 7.
2. Press **UP** or **DOWN** to adjust the display contrast to the desired level.
3. Press **OK**.

If the trouble is with an M7100 telephone

1. Press Feature * 7.
2. Press a number on the dial pad to adjust the display contrast to the desired level.
3. Press Hold.

If the display is still unreadable

1. In the Unified Manager, select **Resources, Telephony** and then **Maintenance**, to disable the problem telephone.

2. Replace the problem telephone with a known working one.

3. Enable the working telephone.

Telephone dead

1. Run a Station Set Test **(**Feature 8 0 5**)**.

2. Check for dial tone.

3. Check the display.

4. If the problem persists, replace the telephone with a known working telephone of the same type (so that the programming is retained).

5. Check the internal wiring at both the modular jack and the distribution cross-connect. A TCM port should have between 15 and 26 V DC across the Tip and Ring when the telephone is disconnected.

6. Check the line cord.

Problems with lines

The troubleshooting problems listed here focus on trouble with making calls or using lines. For more information, refer to one of the following problems:

- Calls cannot be made (but can be received) on page 285
- Dial tone absent on external lines on page 286
- Hung lines at a telephone on page 286
- Auto-answer line rings at a telephone on page 288
- Prime telephone gets misdialed calls on page 289
- Selected lines reads “Not in service” or “Not available” on page 290
- Selected line pool shows “No free lines” on page 290

Calls cannot be made (but can be received)

1. If an incorrect line number or name appears (or if neither appears) on the telephone display, check the programming settings.
   OR
   If the correct line number or name appears on the telephone display, make sure the external lines are properly cross-connected.

2. Check external lines by attaching a test telephone directly on the distribution block.

3. Ensure that the 25-pair cable is properly connected from the EE-DSM to the station set termination.

4. In the Unified Manager, verify that the EE-DSM module is not disabled or unequipped by selecting **Resources, Telephony**, **Maintenance** and accessing **Module/port status**. For more information, refer to Display the module status on page 254.

5. In the Unified Manager, select **Resources, Telephony** and then **Maintenance**, to disable the appropriate ports using the heading **Module/port status**. For more information, refer to Disable a module on page 254.

6. Enable the appropriate ports using the heading **Port/DN status**.

7. If you still cannot make external calls, power down, then power up the system. This should be done after business hours to avoid losing calls.

8. To check the line, contact the telephone company.

Notify service provider of T1 signaling disruption.
Notify your T1 service provider before disconnecting your T1 lines, removing power to your system, or performing any other action that disrupts your T1 signaling. Failure to notify your T1 service provider may result in a loss of T1 service.

Dial tone absent on external lines

1. Check for dial tone using a test telephone at the connections for the external line on the distribution block.

2. Make sure that a trunk module for the line is properly installed in the server or expansion cabinet.

3. Make sure that the hub is properly connected to the MSC card.

4. In the Unified Manager, select **Resources, Telephony** and then **Maintenance**, to ensure that the line is not disabled. See Display the module status on page 254.

Hung lines at a telephone

Line indicators that have been solid for a long time are the only visible indication that lines are hung.

Possible problem

A line that has been redirected using Line Redirection may, under some circumstances, remain busy after a call is over. If this happens, the outgoing line for the redirection also remains busy. You can clear this kind of hung line only at the telephone that was used to redirect the line.

Solution

1. Enter the Button Inquiry feature code (Feature * 0) at the telephone that was used to redirect the line.

2. Press the button of the redirected line.

3. Press **SHOW** or #.

4. Press **DROP** or *.

Both the redirected line and the outgoing line for the redirection should now be cleared.

Possible problem

The supervision and/or disconnect timer programming for the line do not match the settings for the line at the central office.

Solution

Verify in the Unified manager that your programming for the line matches the central office settings.

1. Choose **Resources**, **Telephony**, **Lines**.

2. Select the affected line.

3. Select **Trunk/Line data**.

   The line's programming data is displayed.

4. Verify that the supervision and disconnect timer programming match the settings for the line at the central office.

Possible problem

Lines are still hung after all the above solutions have been investigated or tried out.

Solution

For lines that are hung for any other reason, you will have to run a Maintenance session and disable then re-enable the affected trunk module.

1. Choose **Resources, Telephony**, **Maintenance**, **Module/port status**. Disable the module using the procedure, Disable a module on page 254.

2. Enable the module using the procedure, Enable a module on page 255.

Follow the procedures in the Basic troubleshooting procedure on page 282 before proceeding.

Auto-answer line rings at a telephone

Possible problem

You configured a loop start trunk as auto-answer but the installed hardware does not support disconnect supervision. (In this case, the symptom would be accompanied by the Alarm 62 code symptom.)

Solution

Reconfigure the trunk as manual-answer.

Possible problem

The line is configured as auto-answer and unsupervised.

Solution

Reconfigure the line as manual-answer or reconfigure the line as supervised.

1. Choose **Resources**, **Telephony**, **Lines**.

2. Select the affected line.

3. Select **Trunk/line** data.

4. In the **Trunk mode** field, reconfigure the line as supervised by selecting **Super** from the drop-down menu.

   OR

   In the **Auto answer** field, reconfigure the line as manual answer by selecting **Manual** form the drop-down menu.

Possible problem

The line is not equipped for disconnect supervision at the central office.

Solution

Reconfigure the trunk as manual-answer.

1. Choose **Resources**, **Telephony**, **Lines**.

2. Select the affected line.

3. Select **Trunk/line** data.

4. In the **Auto answer** field, reconfigure the line as manual answer by selecting **Manual** form the drop-down menu.

Possible problem

The disconnect timer setting for the trunk module in **Trunk/Line data** does not match the setting for the line at the central office.

Solution

Reconfigure the disconnect timer in the Unified Manager to match the setting at the central office.

1. Choose **Resources**, **Telephony**, **Lines**.

2. Select the affected line.

3. Select **Trunk/Line data**.

   The data is displayed for this line.

4. In the **Trunk mode** field, select the correct setting from the drop-down menu.

For more information, refer to Trunk mode on page 103.

Prime telephone gets misdialed calls

Possible problem

The digits sent by a switch at a central office or in the private network did not match any Received number or the Auto DN. The call has been routed to the prime telephone for the incoming trunk.

Solution

1. Verify that the switch is sending the correct number of digits for the Received number length defined in your system.

2. Verify all the digit strings that the switch should be sending.

3. Check that you have defined the corresponding Received number for every target line in your system.

4. Make sure that the published telephone numbers for your network are correct.

Selected lines reads “Not in service” or “Not available”

Possible problem

The line is connected to an EE-DTM which is currently not in service.

Solution

1. Check if the green LED on the EE-DTM is flashing to indicate that service is suspended.
2. Check if any yellow LEDs are on to indicate an alarm or error condition.
3. Check if the red test LED is on to indicate that a continuity loopback test is running.
4. Check that the cable connecting the EE-DTM to the termination point from the central office or network is properly connected.
5. Check that the EE-DTM is properly inserted in the module bay.
6. In the Unified Manager verify the status of the EE-DTM. For more information, refer to the procedure, Display the module status on page 254.

Possible problem

The line has been disabled for maintenance purposes.

Solution

Enable the line.
OR
If the line will be out of service for some time, configure another line to replace it on the telephone.

Possible problem

The line has not been provisioned.

Solution

Provision the line.

Selected line pool shows “No free lines”

Possible problem

If this happens often, there are not enough lines in the line pool to serve the number of line pool users.

Solution

If the line pool contains loop start trunks, enter programming and move the under-utilized loop start trunks from other line pools into the deficient line pool.

Problems with optional equipment

For more information on problems with optional equipment attached to the Enterprise Edge system, refer to one of the following problems

- Problems with the Enterprise Edge ATA 2 on page 291
- Problems with the auxiliary ringer on page 292
- Problems with external paging on page 292
- Problems with Music on Hold and Background Music on page 293

Problems with the Enterprise Edge ATA 2

1. Check the connections to the jack.

2. Check the connections to the Enterprise Edge ATA 2.

3. Disconnect the Enterprise Edge ATA 2 and replace it with a working digital telephone. If the telephone still works properly, the system and the EE-DSM are operating properly.

4. Verify that the programming has been performed correctly.

5. If the trouble seems to be in the system or EE-DSM, double-check all wiring and programming options.
   OR
   If the trouble seems to be with the Enterprise Edge ATA 2, disable the Enterprise Edge ATA 2 and replace it with a known working one.

For more information, refer to the *Enterprise Edge ATA 2 Installation Guide*.

Running a Maintenance session to test a Enterprise Edge ATA 2

1. Choose **Resources, Telephony**, **Maintenance**, to ensure that the Enterprise Edge ATA 2 is not disabled. See Identify a device connected to the system on page 255.

2. Disable the port connected to the Enterprise Edge ATA 2 using the procedure, Disable a device on page 256.

3. Enable the port connected to the Enterprise Edge ATA 2 using the procedure, Enable a device on page 257.

Problems with the auxiliary ringer

1. If the auxiliary ringer is used for Schedules (Night, Evening, or Lunch service), ensure that Schedules is activated from the control telephone.

2. Check the wiring between the auxiliary ringer generator and the ringing device. Refer to the auxiliary ringer wiring chart.

3. Check the following wiring between the auxiliary ringer generator and the distribution block:

Feature	Pin
Auxiliary ring (Make)	44 (Yellow-Brown)
Auxiliary ring (Common)	19 (Brown-Yellow)

4. Ensure that the auxiliary ringer contacts are operating properly by checking with an ohmmeter across the auxiliary ringer pin contacts listed above.

5. Check that the auxiliary ringer pin contacts are programmed to operate in conjunction with any or all of the features in the auxiliary ringer programming chart.

Feature	Programmed in
Auxiliary ringer	Terminals&Sets
Auxiliary ringer	Lines
Schedules	Services

The current capacity of the Enterprise Edge relay contacts is 50 mA DC. They are designed to operate with the auxiliary ringer generator, or equivalent.

Problems with external paging

1. Use the Button Inquiry feature **(**Feature * 0**)** to verify the feature of a programmable memory button.

2. Check the wiring between the 50-pin connector and the paging amplifier or between the connections shown in the external paging wiring chart.

Feature	Pin
Page out (Tip)	40 (Black-Slate)
Page out (Ring)	15 (Slate-Black)
Page (Make)	41 (Yellow-Blue)
Page (Common)	16 (Blue-Yellow)

3. Test external paging Feature 6 2 to ensure that it is working. The nominal output signal from the Enterprise Edge is 100 mV across 600 Ω.

Problems with Music on Hold and Background Music

Although Music on Hold and Background Music are separate features, they share the same wiring and customer-supplied music source.

1. Ensure that the proper feature access code **(**Feature 8 6**)** is turned on. Adjust the volume using the volume control bar.

2. Use the Button Inquiry feature **(**Feature * 0**)** to verify the feature on a programmable memory button.

3. If there is trouble with Music on Hold or Background Music, check the feature settings in the Unified Manager by selecting **Resources, Telephony**, **General settings** and then **Feature settings**.

4. Check the wiring between the music source and the 50-pin connector.

5. Ensure that the music source is turned on, is operational, and the volume control is set properly.

6. Any music source with a low-output impedance (for example, less than 3,300 ohms) can be connected. The output level must be less than one volt.

Problems with module service

Check first for user problems, then wiring connections and programming errors before replacing Enterprise Edge equipment.

Notify service provider of T1 or PRI signaling disruption.
Notify your T1 or PRI service provider before disconnecting your T1 or PRI lines, removing power to your system, or performing any other action that disrupts your T1 or PRI signaling. Failure to notify your T1 or PRI service provider may result in a loss of T1 or PRI service.

1. Check that the module is properly inserted in the server or expansion cabinet.

2. Access **Resources, Telephony** and then **Feature settings**, ensure that the module is not disabled. For more information, refer to the procedure, Display the module status on page 254.

If the problem persists
If the AC power is present and the LED indicator on the module is off, contact your customer service representative. If AC power is present and the LED indicator on the Enterprise Edge system is off, replace the system power supply.

Note: Before you replace the system power supply, disconnect all central office and station lines from the Enterprise Edge system. Power down the system by unplugging it.

Refer to *Enterprise Edge Installation and Maintenance Guide* for information on replacing components.

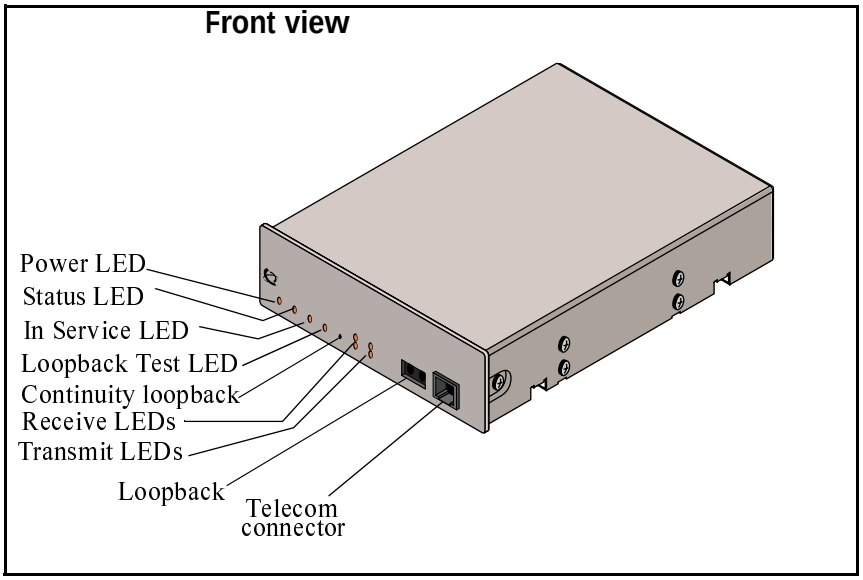
Refer to the following sections for more information:

- Digital Trunk Computer Module trouble on page 294
- Monitoring the T1 or PRI signal on page 295

Digital Trunk Computer Module trouble

1. Choose **Resources, Telephony**, **Maintenance** to verify that the EE-DTM is enabled and that it's lines are provisioned. For more information, refer to the procedure, Display the module status on page 254.

2. Check the LEDs on the front of the EE-DTM



- **Receive Alarm**: yellow LED on indicates a problem with the digital transmission being received. This half-duplex link is unusable.
- **Receive Error**: yellow LED indicates a minor error as a result of degraded digital transmission. Possible causes are an ohmic connection, water ingress, or too long a loop.
- **Transmit Alarm**: red LED on indicates an inability to transmit. Alarm indication signal (AIS) is being transmitted to the terminating switch. This half-duplex link in unusable.
- **Transmit Error**: yellow LED on indicates a remote alarm indication (RAI) carrier failure alarm (CFA) is being sent to the terminating switch. If the Transmit Alarm is not on, this indicates a far-end or cable problem.

- **In service**: flashing green indicates that the T1 or PRI trunks are out of service because of a running loopback test, or because the EE-DTM is being initialized.
- **Loopback test**: red LED on while a continuity loopback test is running.
- **All LEDs flashing continuously**: the EE-DTM is being initialized.

3. In the Unified Manager, select **Resources, Telephony**, **Maintenance**, and **Tests** to run any loopback tests as appropriate.

4. Check the pinout of the cable that connects the EE-DTM to the termination point from the T1 or PRI service provider or the external channel service unit, and check that the cable is properly connected.

5. Check with your T1 or PRI service provider to see if through-fed repeaters are used on the T1 or PRI span. The EE-DTM does not provide the DC connection required for through-fed repeaters. If through-fed repeaters are used on the T1 span, disable the internal CSU and connect the EE-DTM to an external CSU.

6. If the problem persists, replace the EE-DTM.

Notify service provider of T1 or PRI signaling disruption.
Notify your T1 or PRI service provider before disconnecting your T1 or PRI lines, removing power to your system, or performing any other action that disrupts your T1 or PRI signaling. Failure to notify your T1 or PRI service provider may result in a loss of T1 or PRI service.

For information on how to replace any system components, refer to the *Enterprise Edge Installation and Maintenance Guide*

Monitoring the T1 or PRI signal

If you are finding minimal faults with the T1 or PRI signal, you can monitor the signal to try and isolate the problem. The monitor jack on the EE-DTM faceplate provides non-intrusive, bridged in-service monitoring of the T1 or PRI signal. Connect a protocol analyzer or other test equipment into the monitor jack to monitor the signal received from the network, and the signal transmitted by Enterprise Edge.

Problems with Trunk or Station Modules

1. Choose **Resources, Telephony**, **Maintenance** to ensure that the module is not disabled. For more information, refer to the procedure, Display the module status on page 254.

2. Disable the module using the procedure, Disable a module on page 254.

3. Enable the module using the procedure, Enable a module on page 255.

4. For an EE-DTM, EE-CTM or EE-DSM:

   Check the external line by terminating a single-line telephone directly on the distribution block, or equivalent, which connects to the Trunk Module.

5. For the EE-ASM:

   If the EE-ASM is still down, power down, then power up the Enterprise Edge system.

If the problem persists

1. If AC power is present and the LED indicator on the module is off, replace the module.

2. Replace the link cable.

3. Replace the module.

4. Replace the MSC.

For information on replacing components, refer to the *Enterprise Edge Installation and Maintenance Guide*.

Problems for network or remote users

Refer to one of the following items for information on how to solve network or remote user problems.

- Remote feature code gets no response on page 297
- Dialed number gets ringback and the wrong person on page 297
- Dialed number gets dial tone instead of ringback on page 297
- Dialed number gets busy tone on page 298
- Dialed number does not get through on page 298
- Dialed feature code gets overflow tone on page 299
- Dialed feature code gets busy tone on page 300
- Line pool access code gets overflow tone on page 300
- Line pool access code gets ringback on page 301
- Line pool access code gets busy tone on page 301
- Dialed number gets no response on page 301

Remote feature code gets no response

Possible problem

An Enterprise Edge user has called into another Enterprise Edge system and is trying to activate a remote feature but gets no response after dialing the feature code.

Solution

1. Make sure that the remote caller is dialing the feature code correctly. Use the asterisk (*) character, followed by the feature code, to activate a remote feature. (Do not use **Feature** for accessing features on a remote Enterprise Edge system.)

2. Make sure that the remote user is dialing tones, not pulses once the call is answered.

Dialed number gets ringback and the wrong person

Possible problem

The digits sent by a switch at a central office or in the private network did not match any Received number or the Auto DN. The call has been routed to the prime telephone for the incoming trunk.

Solution

1. Verify that the switch is sending the correct number of digits for the Received number length defined in your system.

2. Verify all the digit strings that the switch should be sending.

3. Check that you have defined the corresponding Received number for every target line in your system.

4. Make sure that the published telephone numbers for your network are correct.

Dialed number gets dial tone instead of ringback

Possible problem

The remote caller has tried to reach an Enterprise Edge target line, but has reached the Enterprise Edge system instead. The system has mapped the incoming digits onto the Auto DN.

Solution

1. Verify all the digit strings that the switch should be sending.
2. Check that you have defined the corresponding Received number for every target line in your system.
3. Check that you have defined the correct Auto DN for your system.
4. Make sure that the published telephone numbers for your network are correct.

Dialed number gets busy tone

Possible problem

The target line that the incoming digits map onto is busy, and there is no prime telephone for the incoming trunk.

Solution

For maximum call coverage, make sure that you configure a prime telephone for every incoming trunk.

Dialed number does not get through

Possible problem

The digits sent by a switch at a central office or in the private network did not match any Received number or the Auto DN. There is also no prime telephone assigned for the incoming trunk. In this case, the caller may hear overflow tone from the Enterprise Edge system or a recorded message from the originating switch.

Solution

1. Configure a prime telephone for every incoming trunk.
2. Verify that the switch is sending the correct number of digits for the Received number length defined in your system.
3. Verify all the digit strings that the switch should be sending.
4. Check that you have defined a Received number for every target line in your system.
5. Make sure that the published telephone numbers for your network are correct.

Possible problem

The Enterprise Edge system did not receive some or all of the incoming digits.

Solution

1. Check that the system hardware is receiving signals properly.

2. Verify that the switch is sending the correct number of digits for the Received number length defined in your system.

3. If the switch at the far end is sending pulse signals, make sure they are being sent at the proper rate. (Pulse digits must be 300 ms or more apart for the Enterprise Edge system to receive them.)

Dialed feature code gets overflow tone

Possible problem

The remote caller does not have access to that feature.

Solution

Check the remote package that you assigned to the incoming trunk. Make sure that it gives the appropriate access to the remote caller.

Possible problem

The feature code is not valid.

Solution

1. Make sure that remote callers have a correct listing of the features that are programmed for remote access.

2. Ensure that remote callers are programming the feature code correctly. Press * followed by the feature code to activate a remote feature.

Possible problem

The caller may be dialing on a rotary-dial telephone or on a push-button telephone that uses pulse signaling.

Solution

Inform remote callers that they must dial from a push-button telephone that uses DTMF “tone” signaling.

Dialed feature code gets busy tone

Possible problem

A resource that the remote feature uses may currently be in use. For example, a remote caller trying to use the paging feature would get a busy tone if the auxiliary speaker were being used at the time.

Solution

If repeated attempts to use the remote feature get busy tone, there may be a malfunction in a resource that the feature uses. Check that the remote feature hardware is functioning normally.

Line pool access code gets overflow tone

Possible problem

If the published line pool access code is valid, the remote caller does not have access to that line pool.

Solution

Change the remote package for the incoming trunk so that it permits access to that line pool.
OR
Give the remote caller a line pool access code that is permitted within the Class of Service on the incoming trunk.

Possible problem

If the published line pool access code is invalid, the system has attempted, without success, to match the invalid code to an Enterprise Edge target line internal number, and there is no prime telephone for the auto-answer trunk.

Solution

1. Make sure that the published line pool access codes are correct.

2. Check that the line pool access codes have been entered correctly under **Access codes** in **System programming**.

Possible problem

The caller may be dialing from the network on a rotary-dial telephone or on a push-button telephone that uses pulse signaling.

Solution

Inform remote callers that they must dial from a push-button telephone that uses DTMF “tone” signaling.

Line pool access code gets ringback

Possible problem

The published line pool access code is invalid, and the system has routed the call to the prime telephone for the incoming trunk.

Solution

1. Make sure that the published line pool access codes are correct.

2. Check that the line pool codes have been entered correctly under **Access codes** in **System programming**.

Line pool access code gets busy tone

Possible problem

There are not enough lines in the line pool to serve the number of users.

Solution

If the line pool contains loop start trunks, enter programming and move under used loop start trunks from other line pools into the deficient line pool.
OR
Create a separate line pool for remote users only.

Dialed number gets no response

Possible problem

The remote caller, after accessing a line in a line pool, may have started dialing before the far end was ready to receive digits.

Solution

Instruct remote callers to wait until they hear feedback before entering any digits.

Possible problem

There may be a malfunction in the line that the remote caller accessed.

Solution

If the problem is persistent, check that all lines in the affected line pool are functioning normally.

Possible problem

There may be a malfunction in the system that the caller is trying to reach.

Solution

Inform the operators of the system at the far end that the dialed number is not getting through.

Problems with Companion sets

When there is a problem with a Companion set:

1. Make sure the portable is compatible with Enterprise Edge Voice Messaging Companion Wireless software.

2. Verify that the portable is ON and that the battery is not low.

3. Establish a radio connection to get a dial tone.

4. If there is no dial tone present:

   - verify that a dial tone is available from Enterprise Edge.
   - the portable may not be registered. If this is the case, register the portable again.
   - check that the portable is using the correct registration slot.
   - verify that the portable has been assigned the correct internal number by calling it from another telephone.

Appendix A: Network Examples

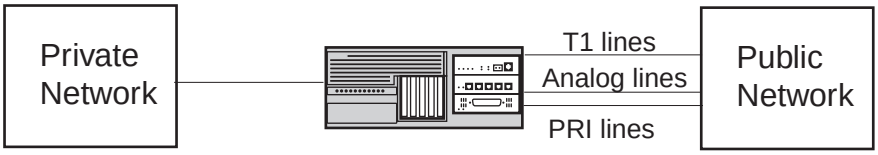
Enterprise Edge in a network

In addition to public network connections, Enterprise Edge can be integrated into an existing private network of M1s to form a corporate telecommunications network.

Tips
The ability to perform private networking requires software keys for Enterprise Edge VoIP Gateway and Enterprise Edge PRI.

The big picture

Enterprise Edge uses enhanced trunking to join other Nortel or customer equipment in a private network. Authorized users can also access tie lines, central office lines, and Enterprise Edge features from outside the system.



Enterprise Edge

Callers using Enterprise Edge can:

- call directly to a specific telephone
- select an outgoing line to access a private network
- select an outgoing line to access features that are available on the private network
- select an outgoing central office line to access the public network
- use all of the Enterprise Edge features.

Callers in the public network can:

- call directly to one or more Enterprise Edge telephones
- call into Enterprise Edge and select an outgoing tie line to access a private network
- call into Enterprise Edge and select an outgoing central office line to access the public network
- call into Enterprise Edge and use remote features.

Callers in the private network can:

- call directly to one or more Enterprise Edge telephones
- call into Enterprise Edge and select an outgoing tie line to access other nodes in a private network
- call into Enterprise Edge and select an outgoing central office line to access the public network
- call into Enterprise Edge and use remote features.

Networking Enterprise Edge with Meridian M1 over PRI

Benefits

Some of the benefits of networking Enterprise Edge and Meridian M1 over PRI include

- common dialing plan
- centralized PSTN trunking (Enterprise Edge users can share the M1's PSTN trunks with M1 users)
- PRI networks can be used for voice, data, and video calls
- no usage costs when placing calls over private networks

Lines

External lines provide the physical connection between Enterprise Edge and other systems in a private or public network. Lines are numbered 061 to 238. Lines 001 to 008 are used for Enterprise Edge VoIP Gateway (IP telephony functionality). Enterprise Edge includes different types of modules that are configured for different types of lines:

- A DTI (EE-DTM) configured for PRI is used for incoming and outgoing calls (two-way DID). Incoming calls are routed directly to an Enterprise Edge telephone. Outgoing calls are made using the intercom key and dialing destination codes.
- A DTI (EE-DTM) configured for T1 has digital lines that are configured as Groundstart, E&M, Loop, and DID.

Target lines are virtual communication paths between trunks and telephones on the Enterprise Edge system. They are incoming lines only, and cannot be selected for outgoing calls.

With target lines, you can concentrate incoming calls on fewer trunks. This type of concentration is an advantage of DID lines, and Enterprise Edge target lines allow you to direct each DID number to one or more telephones. Target lines are numbered 241 to 336.

Telephones can be configured to have an appearance of any type of trunk and line (including target lines, excluding PRI trunks). If assigned, they are used for monitoring call usage.

PRI lines

Primary Rate Interface (PRI) lines give you incoming and outgoing access to an ISDN network and are auto-answer trunks. PRI lines are set to auto-answer by default and cannot be changed. The DTI (EE-DTM) is configured to provide PRI lines.

PRI lines provide a fast, accurate and reliable means of sending and receiving data, images, text and voice information. Using PRI lines allows for faster transmission speeds and the addition of a variety of powerful business applications, including remote LAN access, video conferencing, file transfer and Internet access.

T1 lines (Loop, E&M, DID, Ground start)

Ground start lines offer the same features as loop start trunks, but are used when the local service provider does not support disconnect supervision for the digital loop start trunks. Ground start trunks work with T1 only. By configuring lines as ground start, the system will be able to recognize when a call is released at the far end.

Tips

You cannot change the trunk mode for a ground start trunk on an EE-DTM (or DTI). It always has disconnect supervision.

An EE-DTM configured for T1 can provide a maximum of 24 ground start trunks. Analog ground start trunks are not supported.

Target lines

A target line is a specific communication path that is reached by means of digits received from an incoming trunk. Target lines are used to answer incoming calls but cannot be used to make outgoing calls.

Target lines are assigned by default for all templates except the DID template.Target lines are assigned line numbers (for example, 241 to 336) similar to physical lines.

You can program auto-answer T1 loop start, T1 E&M trunks, T1 DID, T1 ground start trunks, PRI, and IP trunks to map to target lines to provide for attendant bypass (calling directly to a department or individual) and line concentration (one trunk can map onto several target lines).

Remote system access

The remote access feature allows callers elsewhere on the private or the public network to access Enterprise Edge by dialing directly without going through an attendant. Once in the system, the remote user can use some of the system's resources. The remote access must be enabled in programming before callers can use it.

Enterprise Edge supports remote system access on the following trunk types which may require the remote caller to enter a password for direct inward system access (DISA):

- auto-answer loop start trunks
- auto-answer E&M trunks
- DID trunks (by means of the DISA DN)
- PRI trunks (by means of the DISA DN)

The system resources (dialing capabilities, line pool access and feature access) that a remote user may access depends on the Class of Service (COS) assigned to them. See COS passwords on page 130 and the *Nortel Networks Voice Programming Guide* for more details.

To use features on Enterprise Edge remotely, press * followed by the feature code. Even if you are calling from another Enterprise Edge system, press * instead of Feature.

Remote access on loop start trunks

Loop start trunks provide remote access to Enterprise Edge from the public network. They must be configured to be auto-answer to provide remote system access.

A loop start trunk **must** have disconnect supervision if it is to operate in auto-answer mode. T1 E&M trunks always operate in disconnect supervised mode.

When a caller dials into the system on a line that has auto-answer, the system answers with system dial tone and no (COS) password is required. In this case, control over the system capabilities available to the caller is provided only by the restriction filters assigned to the line.

When a caller dials in on a line that has auto-answer with DISA, the system answers with stuttered dial tone. This is the prompt to enter a COS password which determines which system capabilities are available to the caller.

Remote access on a private network

Nodes on the private network deliver the last dialed digits to the destination Enterprise Edge node for interpretation. The destination Enterprise Edge node either matches the digits to a target line or interprets the digits as a remote feature request. The call is either routed to the specified target line, or the remote feature is activated.

By default, T1 E&M trunks are set to answer with DISA. For auto-answer T1 E&M trunks connected to a private network, change the default so that the trunks are **not** answered with DISA.

If an auto-answer T1 E&M trunk is configured to answer with DISA, the system tries to interpret any received digits as a COS password.

The DISA DN and the Auto DN allow auto-answer private network and DID calls, in the same way that calls on auto-answer loop start and auto-answer T1 E&M trunks can be answered, with or without DISA. These DNs are described in **System programming** under **Access codes**.

Remote access on T1 Direct Inward Dial (DID) trunks

Remote system access on T1 DID trunks is similar to that of T1 E&M trunks connected to a private network. The main differences are:

- a remote caller is on the public network dialing standard local or long-distance telephone numbers
- the digits received are delivered by the central office
- DISA cannot be administered to a T1 DID trunk

As with a private network, the dialed digits may be programmed to match those of a specific target line DN, the DISA DN or the Auto DN.

Remote access on PRI trunks

Remote system access on PRI trunks is similar to that of T1 E&M trunks connected to a private network. The main differences are:

- a remote caller is on the public network dialing standard local or long-distance telephone numbers
- the digits received are delivered by the central office
- answer with DISA cannot be administered to a PRI trunk

As with a private network, the dialed digits may be programmed to match those of a specific target line DN, the DISA DN or the Auto DN.

Security

Programming provides several ways of protecting Enterprise Edge from unauthorized access or use.

Class of Service

Class of Service (COS) refers to the capabilities that Enterprise Edge provides to users who access the system from the public or a private network. The COS includes:

- filters that restrict dialing on the line
- an access package, which defines the set of line pools that may be accessed and whether or not the user has access to the paging feature.

The COS that is applied to an incoming remote access call is determined by:

- the filters that you apply to the incoming trunk
- the COS password that the caller used to gain access to Enterprise Edge.

In cases where DISA is not automatically applied to incoming calls, the remote caller can change the COS by dialing the DISA DN and entering a COS password. To program COS passwords, see COS passwords on page 130.

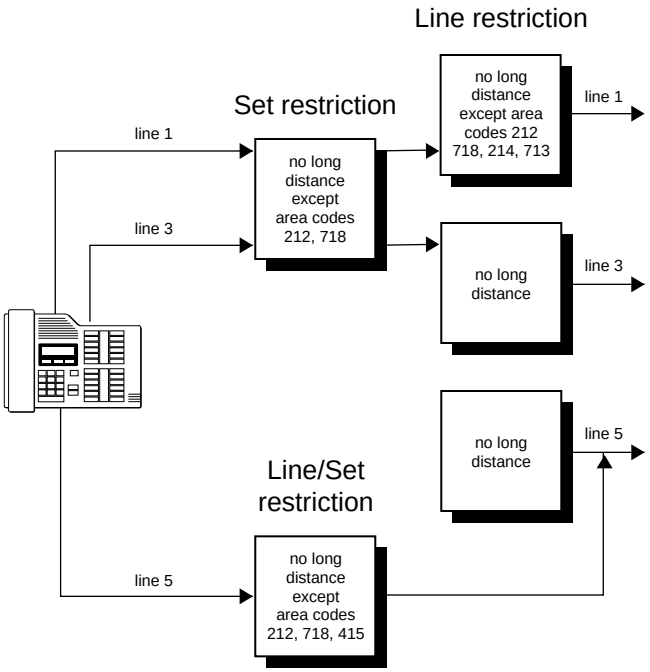
Restriction filters

Restriction filters can be used to restrict the numbers that may be dialed on any external line within Enterprise Edge. Up to 100 restriction filters can be created for the system. A restriction filter consists of up to 48 restrictions and their associated overrides.

To restrict dialing within the system, you can apply restriction filters to:

- outgoing external lines (as line restrictions)
- telephones (as set restrictions)
- external lines on specific telephones (as line/set restrictions)

Restriction filters can also be specified in Restrictions service for times when the system is operating according to a schedule. See Restriction service on page 114 for more details.

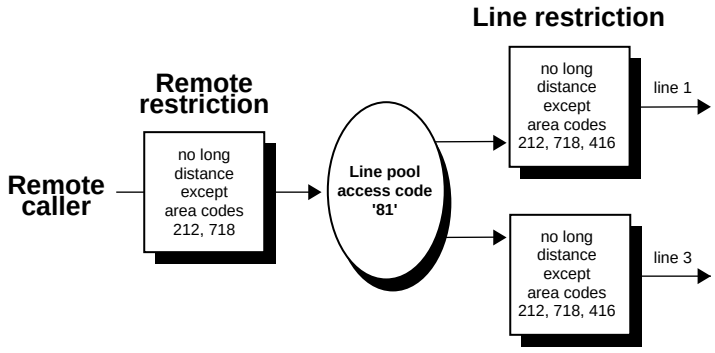


Dialed digits must pass both the line restrictions and the set restrictions. The line per set (line/set) restriction overrides the line restriction and set restriction.

In this diagram, a caller using line 001 could only dial long-distance numbers to area codes 212 and 718. A caller using line 003 could not dial any long-distance numbers. A caller using line 005 could dial long-distance numbers to area codes 212, 718, and 415.

Tip

To restrict dialing from outside the system (once a caller gains remote access), apply restriction filters to incoming external lines (as remote restrictions).


Line restriction
Remote restriction
Remote caller
no long distance except area codes 212, 718
Line pool access code '81'
no long distance except area codes 212, 718, 416
no long distance except area codes 212, 718, 416
line 1
line 3

In this case, dialed digits must pass both the remote restriction and the line restriction. A remote caller can override these filters by dialing the DISA DN and entering a COS password.

For restriction filter programming instructions, see Restriction filters on page 108 in this guide.

Direct inward system access (DISA)

To control access from the public or private network, you can configure auto-answer trunks to answer with DISA. Remote callers hear a stuttered dial tone and must then enter a COS password that determines what they are allowed to do in the system.

Auto-answer T1 loop start and T1 E&M trunks are configured to answer with DISA by default. For DISA programming instructions, see Answer with DISA on page 103.

Tips

T1 DID trunks cannot be configured to answer with DISA. If you want incoming T1 DID calls to be answered with DISA, configure the system with a DISA DN. Incoming T1 DID calls that map onto the DISA DN are then routed to a line that has DISA.

For DISA programming instructions, see Answer with DISA on page 103.

Coordinated dialing plan

Enterprise Edge has a routing feature that allows you to set up a coordinated dialing plan with other systems in the public network. The goal is to have a network-wide dialing plan where all telephone numbers are unique and of a uniform length.

Coordinated dialing plans are typically used with a network of systems with a three to seven digit dialing access between them.

Any programming for routing should be carefully planned using tables. For more information about routing and destination codes, see Routing service on page 114. This section deals with applying the programming in network situations.

Coordinated dialing plan using public lines

The following illustrations provide an example of how you might record dialing plan information in a spreadsheet. The example shows dialing plan information for a Toronto system in a network of three offices: Toronto, Halifax and Vancouver. Without routing, an Enterprise Edge user in Toronto would have to select a line pool and dial 1-902-585-3027 to reach extension 27 in Halifax (902). By creating a destination code of 30 and creating a route that uses the proper line pool and dial out number (referred to as “External #” in programming), the user simply dials 3027. The same feature is available for Vancouver (604).

In the column Dial out, P stands for pause, a host system signaling option. Press Feature 7 8 to insert a 1.5 second pause in the dialing string.

Routing Service (Services: Routing Service)

Route # (000-999)	Dial out (if required) (max. 24 digits or characters)	Use Pool
100	1-P-902-585	A B C
101	1-P-902-585	A B C
102	1-P-604-645	A B C
103	1-P-604-645	A B C
		A B C

Routing service (continued)

Dest code (Services: Routing service: Dest codes)

Service Schedule	Normal		Sched 1		Sched 2		Sched 3	
Sched name (max. 7 char.)	Normal		Night		Evening		Lunch	
DestCode (max. 7 digits)	Use route (001-999)	Absorb Length	Use route (001-999)	Absorb Length	Use route (001-999)	Absorb Length	Use route (001-999)	Absorb Length
30	100	0	000	All	000	All	000	All
31	101	0	000	All	000	All	000	All
32	102	0	000	All	000	All	000	All
33	103	0	000	All	000	All	000	All

Destination code numbering in a network

Because the system checks the initial digits of a call against the routing tables, each type of internal or external call must begin with a unique pattern of digits. The following table gives a sample plan for how initial digits are assigned in a network of systems with three-digit intercom numbers.

Leading Digits	Use
0	Network Direct Dial
221-253	Intercom calls
4	Coordinated Dialing Plan
5	Unused
6	Unused
8	Call Park Prefix
9	All PSTN Calls

In the table, 4 is used as the initial digit for the coordinated dialing plan, but 5, or 6 could also be used for this purpose.

Tip

When programming a button to dial a Network number automatically (autodial), network calls must be programmed as external autodial numbers, even though they resemble internal extension numbers.

Routes generally define the path between the Enterprise Edge system and another switch in the network, not other individual telephones on that switch.

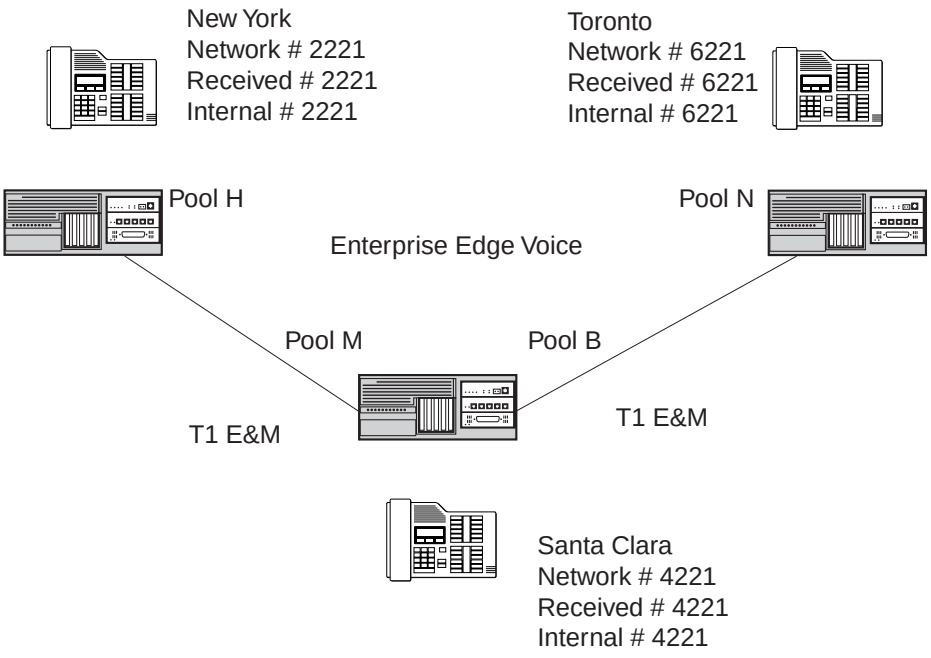
Dialing plan using T1 E&M lines

By properly planning and programming routing tables and destination codes, an installer can create a dialing plan where:

- T1 E&M lines between Enterprise Edge systems are available to other systems in the network

The following figure and programming chart shows a coordinated dialing plan for a network of three Enterprise Edge systems. Each system must be running Enterprise Edge software. Each system must be equipped with target lines and Enterprise Edge with an EE-DTM with at least one T1 E&M line.

Routing by destination codes



Heading	Parameter	Setting
New York office:		
Trunk/Line Data	Line 061	T1 E&M
	Answer Mode	Auto
	Line type	Pool H
	Line 241	Target line
	Received #	2221
Line Access	Set 2221	L241: Ring only
	Line pool access	Line pool H
To Santa Clara:		
Routing service	Route	001
	Use	Pool H
	External #	None
	Destination Code	4
	Normal route	001
	Absorb	None
To Toronto:		
Routing service	Destination Code	6
	Absorb	None
	Normal route	001
Santa Clara office:		
Trunk/Line Data	Line 091	T1 E&M
	Answer Mode	Auto
	Line type	Pool M
Trunk/Line Data	Line 092	T1 E&M
	Answer Mode	Auto
	Line type	Pool B
	Line 251	Target line
	Received #	4221
Line Access	Set 4221	L251: Ring only
	Line pool access	Line pool B Line pool M
To New York:		
Routing service	Route	001
	Use	Pool M
	External #	None
	Destination Code	2
	Absorb	None
	Normal route	001

Heading	Parameter	Setting
To Toronto:		
Routing service	Route	002
	Use	Pool B
	External #	None
	Destination Code	6
	Absorb	None
	Normal route	002
Remote access	Rem access pkgs	01
	Line pool access	Pool M: ON
	Rem access pkgs	02
	Line pool access	Pool B: ON
	Line abilities	049
	Remote pkg	01
	Line abilities	050
	Remote pkg	02
Toronto office:		
Trunk/Line Data	Line 093	T1 E&M
	Answer Mode	Auto
	Line type	Pool N
	Line 300	Target line
	Received #	6221
Line Access	Set 6221	L300: Ring only
	Line pool access	Line pool N
To New York:		
Routing service	Route	001
	Use	Pool N
	External #	None
	Destination Code	4
	Absorb	None
	Normal route	001
To Santa Clara:		
Routing service	Destination Code	2
	Absorb	None
	Normal route	001

If a user in New York wishes to call Toronto within the network, they dial 6221. The local Enterprise Edge checks the number against the routing tables and routes the call according to the destination code 6, which places the call using Route 001.

The call appears on the auto answer line on the Enterprise Edge in Santa Clara as 6-221. Because 6 is programmed as a destination code for Toronto on the Santa Clara system, another call is placed using route 002 from Santa Clara to Toronto. At the Toronto system, the digits 6-221 are interpreted as a target line received number. The call now alerts at telephone 6221 in Toronto.

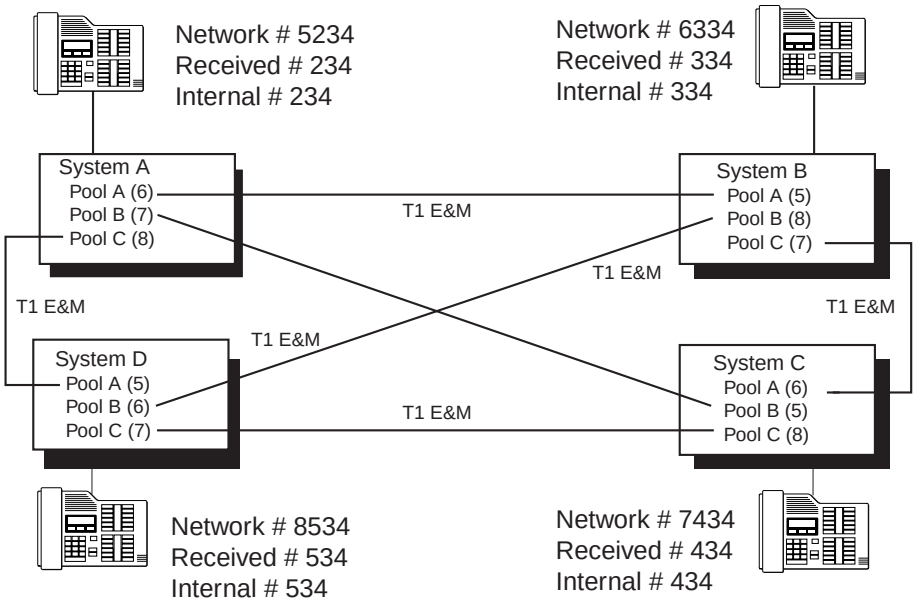
Dialing plans with shared line pools

Using routes and destination codes is a powerful and efficient way to create a coordinated dialing plan. Line pools offer an alternate method of creating a dialing plan or supplementing the routing and destination codes.

If the Enterprise Edge systems are close to each other geographically, you can conserve resources by not duplicating access. For example, system A, B, and C are all within the same area code. System A has a line pool to Santa Clara, System B has a line pool to Montreal, and system C has a line pool to Miami. An Enterprise Edge user in system A can reach Miami by calling system C and using their line pool to Miami.

To simplify access between Enterprise Edge systems, all line pools that go to the same destination should have the same line pool access code. For example, system A and system B both have a line pool to Ottawa. You can configure both systems with the same line pool access code for the Ottawa line pool.

A dialing plan similar to the one in the following figure will let you create a company directory that uses line pool access codes and unique DNs of a uniform length.



For instance, the person on system A at telephone 234 can press an Intercom button and dial 7434.

This means that telephone 234 has dialed the line pool access code of the trunk to system C, and will receive the dial tone of system C. The digits 434 then map to the Received number 434, and ring telephone 434 with an appearance of the associated target line.

Tips

Network calls that use routes are subject to any restriction filters that are in effect.

If the telephone used to make a network call has an appearance of a line used by the route, the call will move from the intercom button to the line button.

The telephone used to make a network call must have access to the line pool used by the route.

Network calls are external calls, even though they are dialed as if they were internal calls. Only the features and capabilities available to external calls can be used.

When programming a button to dial a Network number automatically (autodial), network calls must be treated as external numbers, even though they resemble internal set numbers.

Routes generally define the path between your Enterprise Edge switch and another switch in your network, not other individual telephones on that switch.

For dialing plan information with PRI, see Using a dialing plan to route outgoing PRI calls on page 123.

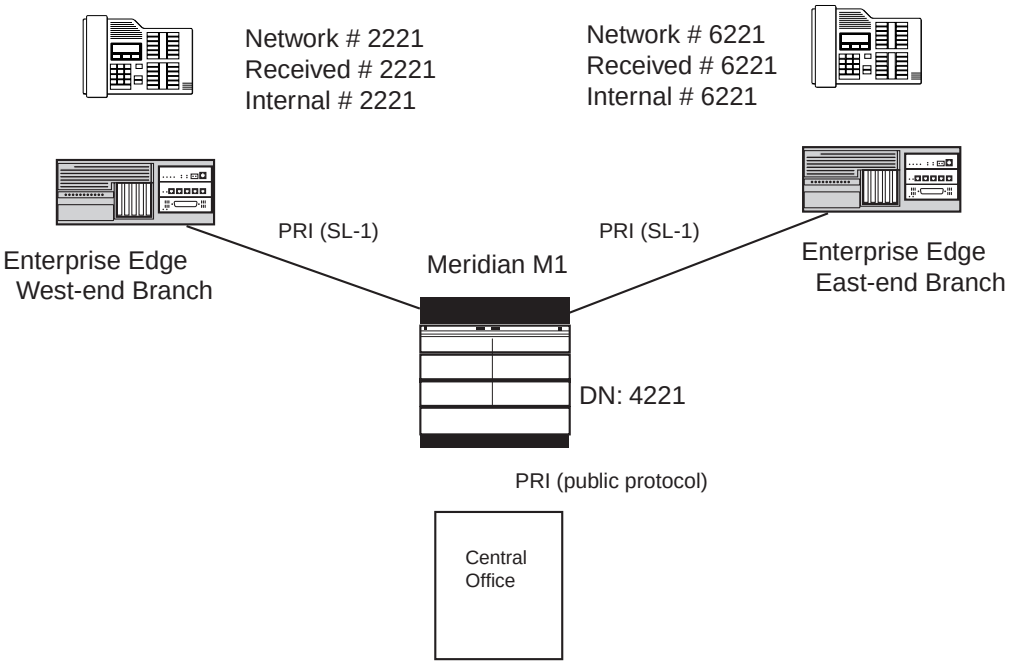
PRI Networking with Meridian 1

Note: Private networking requires an Enterprise Edge PRI software keycode.

This example shows a private network composed of one central Meridian 1, and two smaller sites with Enterprise Edge systems. This could represent a large head office (with the Meridian 1) connected to several smaller branch offices.

In this network, only the head office has trunks connected to the public network. The branch offices access the public network via the private connection to the head office. This configuration allows for cost savings by consolidating the public access trunks. Users at all three locations access the public network by dialing ‘9’, followed by the public number. For example, a user in the west end branch might dial 9-555-1212 (for a local call) or 9-1-613-555-1212 (for a long distance call). These public calls are routed to the Meridian 1 by the Enterprise Edge routing table. Routing tables at the Meridian 1 will then select an appropriate public facility for the call.

Private network calls are made by dialing a 4-digit private network DN. For example, if a user in the west end branch wishes to call a user in the east end branch within the private network, they dial 6221.



In the table that follows, private network routing information is highlighted in gray. Public network routing information is shown in white.

Heading	Parameter	Setting
West End office:		
Hardware	EE-DTM	PRI
	Protocol	SL-1
	BchanSeq	Ascend
	ClockSrc	Primary
Trunk/Line Data	Line 245	Target line
	Received #	2221
Line Access	Set 2221	L245:Ring only
	Line pool access	Line pool PRI-A
To Head Office:		
Routing Service	Route	001
	External #	No number
	Use	Pool PRI-A
	DN type	Private
	Destination Code	4
	Normal route	001
	Absorb	0
To East End:		
Routing Service	Destination Code	6
	Normal route	001
	Absorb	0

Heading	Parameter	Setting
To Public Network:		
Routing Service	Route	002
	External #	No number
	Use	Pool PRI-A
	DN type	Public
	Destination Code	9
	Normal route	002
	Absorb	0
East End office:		
Hardware	EE-DTM	PRI
	Protocol	SL-1
	BchanSeq	Ascend
	ClockSrc	Primary
Trunk/Line Data	Line 245	Target line
	Received #	6221
Line Access	Set 6221	L245:Ring only
	Line pool access	Line pool PRI-A
To Head Office:		
Routing Service	Route	001
	External #	No number
	Use	Pool PRI-A
	DN type	Private
	Destination Code	4
	Normal route	001
	Absorb	0
To West End:		
Routing Service	Destination Code	2
	Normal route	001
	Absorb	0
To Public Network:		
Routing Service	Route	002
	External #	No number
	Use	Pool PRI-A
	DN type	Public
	Destination Code	9
	Normal route	002
	Absorb	0

Additional Configuration

In this example, outgoing public network calls dialed from an Enterprise Edge set are passed to the Meridian M1, and the Meridian M1 is responsible for seizing a public trunk. For this reason, the ‘9’ prefix is left in the number passed to the Meridian 1.

This necessitates that the Public DN lengths table on each Enterprise Edge be modified to account for the extra leading digit. Essentially, the eight pre-configured entries are modified to include a leading ‘9’ in the prefix digits, and the length value for each entry is increased by one. The new entries are listed below. Note that regulatory requirements may demand an entry for 911.

Prefix	Length
Default	8
90	12
900	13
901	18
9011	19
91	12
9411	4
9911	4

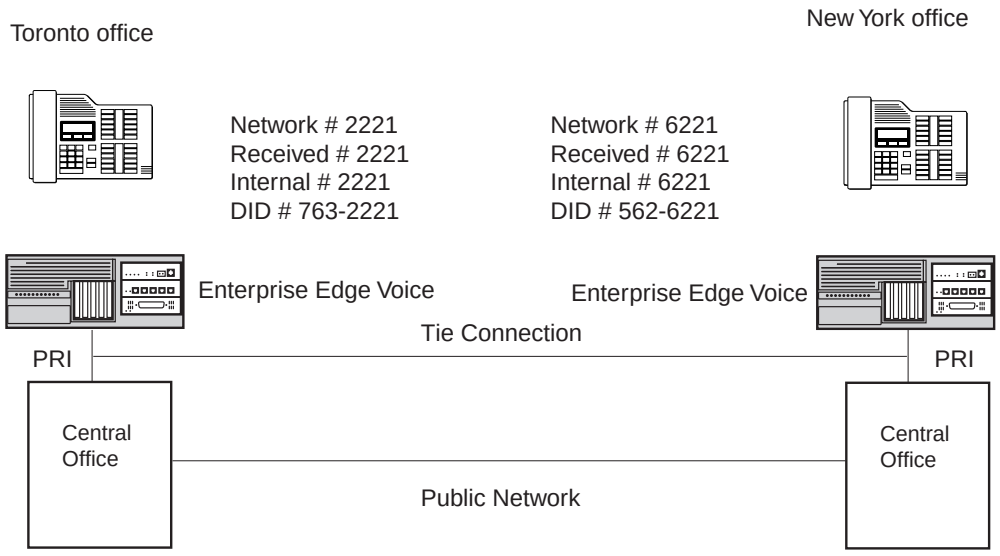
Meridian M1 Configuration

- Meridian M1 is the timing master for the private network PRI connections.
- Meridian M1 uses descending mode for PRI B-channel selection.
- The Meridian M1 must recognize calls dialed to 2xxx and 6xxx numbers, and route the call over PRI to either the East or West end offices. The same applies to incoming DID calls from the public network.
- The Meridian M1 must recognize numbers starting with ‘9’ as public numbers, whether the numbers are dialed by Meridian M1 users or by Enterprise Edge users.

Call-by-Call Services Example

This example highlights the use of PRI Call-by-Call Services.

It shows two offices of a company, one in New York and one in Toronto. Each office is equipped with an Enterprise Edge system and a PRI line. Each office has to handle incoming and outgoing calls to the public network. In addition, employees at each office often have to call colleagues in the other office. To reduce long-distance costs, and to allow for a coordinated dialing plan between the offices, private lines are used to handle inter-office traffic.



If call-by-call services were *not* used, each Enterprise Edge system might have to be equipped with the following trunks:

- 12 T1 DID lines needed to handle peak incoming call traffic.
- 8 T1 E&M lines needed to handle inter-office calls.
- 8 lines needed to handle outgoing public calls

The total required is thus 28 lines. If the Enterprise Edge systems were using T1 trunks, then two T1 spans would be required at each office. Note that the total of 28 lines represents the worst case value for line usage. In reality, the total number of lines in use at any one time will generally be less than 28. For example, during periods of peak incoming call traffic, the demand for outgoing lines will be low.

With PRI call-by-call services, it is not necessary to configure a fixed allocation of trunks. Each of the 23 lines on the PRI can be used for DID, private Tie, or outgoing public calls. This consolidation means that it may be possible for each office to use a single PRI span, rather than two T1 spans. With PRI call-by-call services, the only limitation is that there are no more than 23 calls in progress at any one time.

The dialing plan at each Enterprise Edge site is configured to determine the call type based on the digits dialed by the user. If a user in Toronto wishes to dial a colleague in New York, they dial the 4-digit private DN (such as 6221). The dialing plan recognizes this as a private network DN, and routes the call using Tie service with a private numbering plan.

Incoming Tie calls are routed to sets based on the digits received by the network, which in this case will be the 4-digit private DN.

If a user in either location wishes to dial an external number, they dial ‘9’, followed by the number (such as 9-555-1212). The dialing plan recognizes this as a public DN, and routes the call using Public service.

Incoming DID calls will be routed to sets based on the trailing portion of the digits received by the network. For example, if a public network user dials an employee in the Toronto office, the network will deliver digits 4167632221. Enterprise Edge will route the call using the last four digits, 2221.

In the table that follows, private network routing information is highlighted in gray. Public network information is shown in white.

Heading	Parameter	Setting
Toronto office:		
Hardware	EE-DTM	PRI
	Protocol	NI-2
Trunk/Line Data	Line 245	Target line
	Received #	2221
Line Access	Set 2221	L245:Ring only
	Line pool access	Line pool PRI-A
To New York:		
Routing Service	Route	001
	External #	No number
	Use	Pool PRI-A
	Service type	Tie
	ServiceID	1
	DN type	Private
	Destination Code	6
	Normal route	001
	Absorb	0
To Public Network:		
Routing Service	Route	002
	External #	No number
	Use	Pool PRI-A
	Service type	Public
	Destination Code	9
	Normal route	002
	Absorb	ALL
New York office:		
Hardware	EE-DTM	PRI
	Protocol	NI-2
Trunk/Line Data	Line 245	Target line
	Received #	6221
Line Access	Set 6221	L245:Ring only
	Line pool access	Line pool PRI-A

Heading	Parameter	Setting
To Toronto:		
Routing Service	Route	001
	External #	No number
	Use	Pool PRI-A
	ServiceType	Tie
	ServiceID	1
	DN type	Private
	Destination Code	2
	Normal route	001
	Absorb	0
To Public Network:		
Routing Service	Route	002
	External #	No number
	Use	Pool PRI-A
	Service type	Public
	Destination Code	9
	Normal route	002
	Absorb	ALL

Enterprise Edge VoIP Gateway and M1 networking

This example shows a private network composed of one central Meridian 1, and two smaller sites with Enterprise Edge systems connected over IP trunks through a corporate IP network. This could represent a large head office (with the Meridian 1) connected to several smaller branch offices.

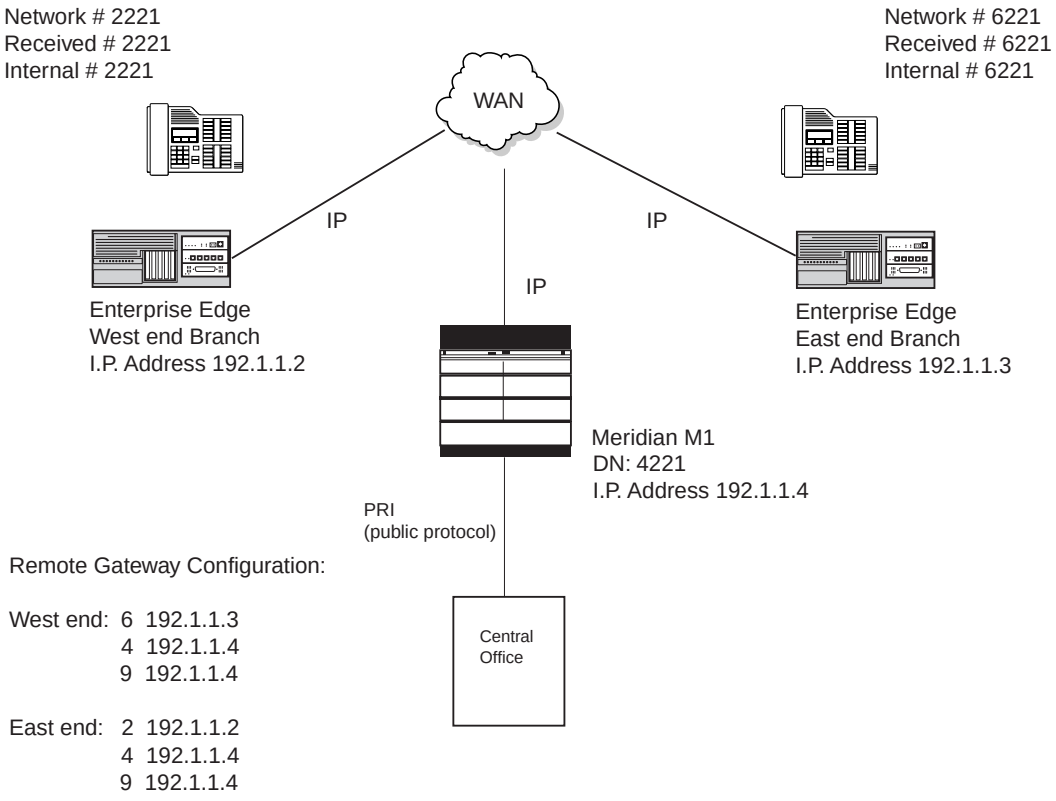
In this network, only the head office has trunks connected to the public network. The branch offices access the public network using IP trunks to the head office. This configuration allows for cost savings by consolidating the public access trunks. Users at all three locations access the public network by dialing ‘9’, followed by the public number. For example, a user in the west end branch might dial 9-555-1212 (for a local call) or 9-1-613-555-1212 (for a long distance call). These public calls are routed to the Meridian 1 by the Enterprise Edge routing table. Routing tables at the Meridian 1 will then select an appropriate public facility for the call.

Private network calls are made by dialing a 4-digit private network DN. For example, if a user in the west end branch wishes to call a user in the east end branch within the private network, they dial 6221.

Note: The quality of the IP trunk connection is assessed during initial call setup, and if the quality is poor, Enterprise Edge will try to find an alternate route to complete the call (fallback) based on the programming definitions in the routing table. For simplicity, this example does not show programming for fallback. In this example, if the quality of the IP connection is considered too low during the call setup phase, the call would fail. For an example of fallback programming, see Toll bypass with Enterprise Edge VoIP Gateway on page 325.

Note: Enterprise Edge VoIP Gateway requires a software keycode.

In the table that follows, private network routing information is highlighted in gray. Public network routing information is shown in white.



The Call Managers examine the Called Party Number digits and route the call to the corresponding IP address.

Heading	Parameter	Setting
West End office:		
Trunk/Line Data	Line 241	Target line
	Received #	2221
Line Access	Set 2221	L241:Ring only
	Line pool access	Line pool A
To Head office (M1):		
Service/Routing Service	Route	001
	Use	Pool A
	External #	(leave blank)
	DN type	Private
	Destination Code	4
	Normal route	001
	Absorb	None
To East End:		
Service/Routing Service	Destination Code	6
	Normal route	001
	Absorb	None
To Public Network:		
Service/Routing Service	Route	002
	Use	Pool A
	External #	(leave blank)
	DN type	Public
	Destination Code	9
	Normal route	002
	Absorb	None
East End office:		
Trunk/Line Data	Line 241	Target line
	Received #	6221
Line Access	Set 6221	L241:Ring only
	Line pool access	Line pool A
To Head Office: (M1)		
Service/Routing Service	Route	001
	Use	Pool A
	External #	(leave blank)
	DN type	Private
	Destination Code	4
	Normal route	001
	Absorb	None

Heading	Parameter	Setting
To West End:		
Service/Routing Service	Destination Code	2
	Normal route	001
	Absorb	None
To Public Network:		
Service/Routing Service	Route	002
	Use	Pool A
	External #	(leave blank)
	DN type	Public
	Destination Code	9
	Normal route	002
	Absorb	None

In this example, outgoing public network calls dialed from an Enterprise Edge set are passed to the Meridian M1, and the Meridian M1 is responsible for seizing a public trunk. For this reason, the "9" prefix is left in the number passed to the Meridian 1.

Note: Ensure that Line Pool A is used for IP trunks.

In order for the digit counting algorithm for outgoing IP calls to take into account this extra digit, the Private Network Access Code must be set to "9" on each Enterprise Edge system.

The Meridian M1 must recognize incoming 2xxx and 6xxx DID calls, and route the call over IP trunks to either the East or West end offices.

The Meridian M1 must recognize numbers starting with "9" as public numbers, whether the numbers are dialed by Meridian M1 users or by Enterprise Edge users.

Toll bypass with Enterprise Edge VoIP Gateway

This example shows a private network composed of one Enterprise Edge system in Toronto and one Enterprise Edge system in Ottawa, connected over IP trunks through a corporate IP network.

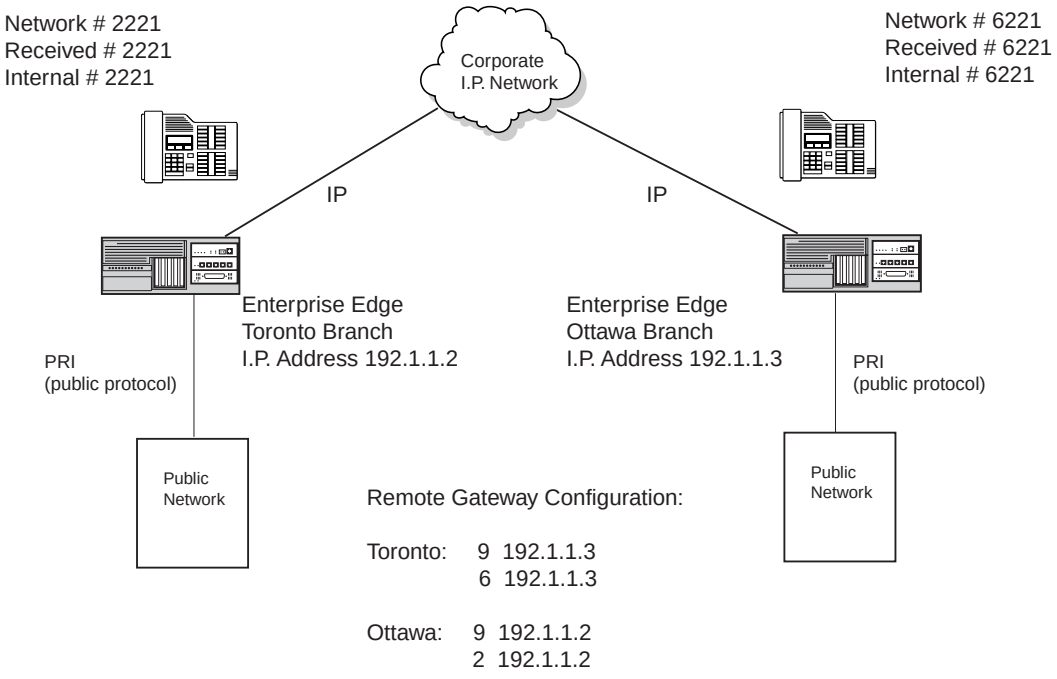
In this network, each Enterprise Edge system has a PRI trunk to the Central Office, and IP trunks to the other Enterprise Edge system. Calls from the Toronto system to the Ottawa system and the Ottawa public network are made over IP trunks with fallback to the PRI trunks when IP trunks are congested. This configuration allows for cost savings by using the corporate IP network whenever possible, thereby bypassing toll charges that would be incurred by using the public network.

Note: When a call gets rerouted over the PSTN due to congestion, the user may see a prompt "Expensive route." The warning indicates that toll charges may be applied to this call.

Users at both locations access the public network by dialing “9”, followed by the public number. For example, a user in Toronto might dial 9-555-1212 (for a local call), or 9-1-613-555-1212 (for a long distance call to Ottawa). Local calls would be sent directly to the Central Office over PRI trunks. Long distance calls to Ottawa would be sent over IP trunks; the Ottawa system would tandem these calls to the local Central Office over PRI trunks.

Private network calls are made by dialing a 4-digit private network DN. For example, if a user in Toronto wants to call a user in Ottawa within the private network, they dial 6221.

Note: Enterprise Edge VoIP Gateway requires a software keycode.



The Call Manager at the Toronto office examines the Called Party Number digits and determines that it should be routed to the IP address corresponding to the Ottawa office. The Ottawa office receives the call, sees that the leading digit(s) match its Private Network Access Code, and uses a destination code to route the call over its public trunks to the PSTN.

This is a simplified example where only calls to the 613 Area Code are routed by the Ottawa node. In a real world configuration, it would also be desirable to handle Area Codes that are ‘close’, for example Montreal: 514.

In the table that follows, private network routing information is highlighted in gray. Public network routing information is shown in white.

Heading	Parameter	Setting
Toronto office:		
Lines/Trunk/Line Data	Line 241	Target line
	Received #	2221
Terminals & sets/Line Access	Set 221	L241:Ring only
	Line pool access	Line pool A Line pool PRI-A
Calls to Ottawa office:		
Services/Routing Service	Route	001
	Use	Pool A
	External #	(leave blank)
	DN type	Private
Services/Routing Service	Route	002
	Use	Pool PRI-A
	External #	(leave blank)
	DN type	Private
Services/Routing Service	Destination Code	6
	Schedule 4	001
	Absorb	None
	Normal route	002
	Absorb	None
Calls to Ottawa Public Network:		
Services/Routing Service	Route	003
	Use	Pool A
	External #	(leave blank)
	DN type	Public
	Route	004
	Use	Pool PRI-A
	External #	(leave blank)
	DN type	Public
	Destination Code	91613
	Normal route	004
	Absorb	1
	Schedule 4	003
	Absorb	None

Heading	Parameter	Setting
To Public Network:		
Services/Routing Service	Destination Code	9161A
	Normal route	004
	Absorb	1
	Destination Code	916A
	Normal route	004
	Absorb	1
	Destination Code	91A
	Normal route	004
	Absorb	1
	Destination Code	9A
	Normal route	004
	Absorb	1
Ottawa office:		
Trunk/Line Data	Line 241	Target line
	Received #	6221
Line Access	Set 6221	L241:Ring only
	Line pool access	Line pool A Line pool PRI-A
To Toronto office:		
Services/Routing Service	Route	001
	Use	Pool A
	External #	(leave blank)
	DN type	Private
	Route	002
	Use	Pool PRI-A
	External #	(leave blank)
	DN type	Private
	Destination Code	2
	Normal route	002
	Absorb	None
	Schedule 4	001
	Absorb	None

Heading	Parameter	Setting
To Toronto Public Network:		
Services/Routing Service	Route	003
	Use	Pool A
	External #	(leave blank)
	DN type	Public
Services/Routing Service	Route	004
	Use	Pool PRI-A
	External #	(leave blank)
	DN type	Public
	Destination Code	91416
	Normal route	004
	Absorb	1
	Schedule 4	003
	Absorb	None
To Public Network:		
Services/Routing Service	Destination Code	9141A
	Normal route	004
	Absorb	1
	Destination Code	914A
	Normal route	004
	Absorb	1
	Destination Code	91A
	Normal route	004
	Absorb	1
	Destination Code	9A
	Normal route	004
	Absorb	1

The implications on the configuration on each node are:

- each node must have the Private Network Access Code set to the value 9.
- each node must have destination code(s) that match the Private Network Access Code plus digits corresponding to calls terminating in the local PSTN. For example, if the Private Network Access Code is ‘9’, the node in Ottawa would require a destination code of ‘91613’. Similarly, Toronto would require the following destination code: 91416.

Note: Ensure that Line Pool A is used for IP trunks.

To allow for fallback to PRI trunks when the IP trunks are congested, you must also program the following Routing service settings:

- Set the start and end times for Sched 4 to 1:00 so that IP calls can be made 24 hours a day.

- Program the Sched 4 Service setting to Auto and enable overflow routing by changing the Overflow setting to Y (Yes).
- A control set must be defined for all sets on the system that make calls over IP trunks. See Control sets on page 126 for more information.

You must program Remote Packages so that the IP trunks in Pool A can access the lines in Pool PRI-A in a toll bypass scenario. In other words, you must give package 01 access to pool PRI-A and you must assign package 01 to all IP trunks. For more information, see Remote access packages on page 146.

Other networking examples

This section shows sample configurations for different types of network access. Each example has four parts:

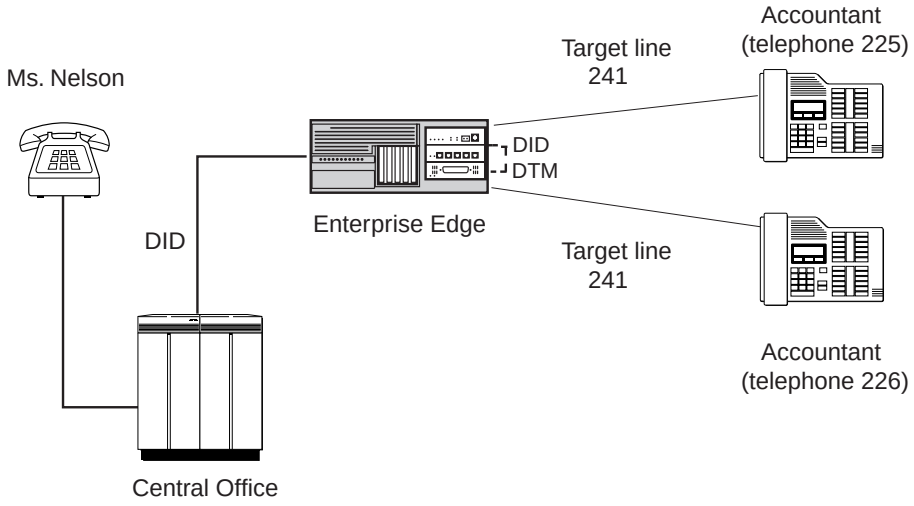
- A scenario explains the caller's goal and what is required to achieve it.
- A diagram shows the network configuration that supports the application.
- A list shows the Enterprise Edge hardware required to support the configuration.
- Tables show the programming required. Only those settings that are important to network access are described here.

Note: The ability to perform private networking is only available with Enterprise Edge software keycodes.

Public network

Call one or more Enterprise Edge telephones

Ms. Nelson is a bank customer who has a question for an accountant. She dials the telephone number 555-4321 that maps onto target line 241. All of the accountants' telephones ring.

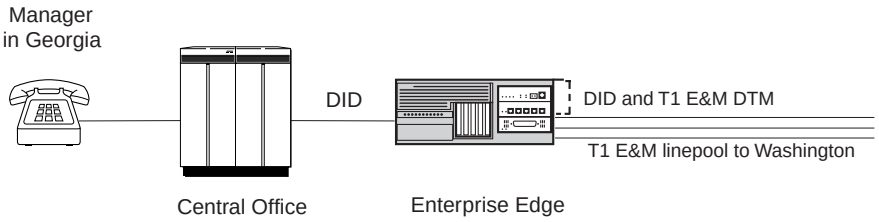


Hardware: Enterprise Edge, an EE-DTM with lines programmed as DID.

Heading	Parameter	Setting
Trunk/Line Data	Received # Line 061	4321 (for Line 241) T1 DID
Rec'd # length	Received # length	4 digits (can be from 2 to 7 digits, but must match number of digits sent by central office)

Call Enterprise Edge and select tie lines to a private network

A manager in Georgia wants to use the tie lines at headquarters to call Washington. He dials a telephone number 555-5321 that maps onto the DISA DN, enters a Class of Service (COS) password, then dials a line pool access code to select a tie line to Washington.

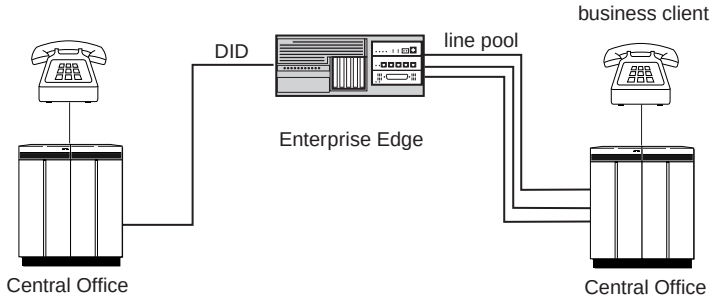


Hardware: Enterprise Edge, an EE-DTM with one T1 DID line and three T1 E&M lines.

Heading	Parameter	Setting
Incoming trunk: Trunk/Line Data	Line 061	T1 DID
Access codes	DISA DN	5321
Rec'd # length	Rec'd # length	4 digits (can be from 2 to 7 digits, but must match number of digits sent by central office)
Outgoing trunk: Trunk/Line Data	Line 062 Line type	T1 E&M Pool F
Access codes	Line pool F	6 (up to 4 digits)
COS pswds		Define restrictions. Define remote access pkgs. Assign a restriction filter to the line. Assign COS passwords and filters for each Class of Service.

Call Enterprise Edge and select lines to the public network

Gord is working from home, and needs to make a long-distance business call from home. To avoid being charged, he dials the telephone number 555-4321 that maps onto the Auto DN at work. After hearing the dial tone, Gord dials a line pool access code 1234 to select a line to the public network. He then dials the long-distance number.



Hardware: Enterprise Edge, EE-DTM with several T1 DID lines.

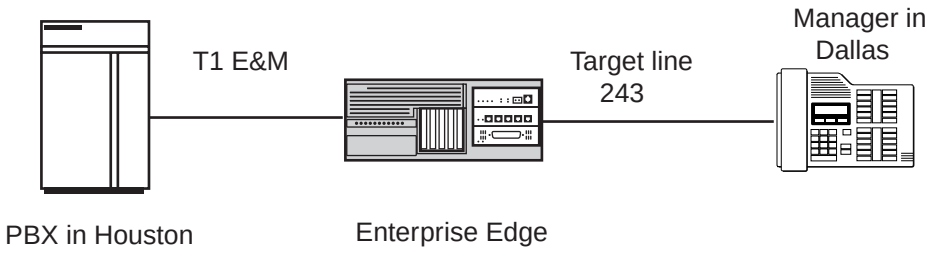
Heading	Parameter	Setting
Incoming trunk: Trunk/Line Data	Line 061	T1 DID
Access codes	Auto DN	4321
Rec'd # length	Rec'd # length	4 digits (can be from 2 to 7 digits, but must match number of digits sent by central office)

Heading	Parameter	Setting
Lines /Restrictions and Remote access		Define restriction filters. Define remote access packages. Assign a remote restriction and remote package to the line.
Outgoing trunk: Trunk/Line Data	 Line 001 Line type	 Loop Pool A
Access codes	Line pool A	1234
Lines /Restrictions		Assign a restriction filter to the line.

Private network

Call one or more Enterprise Edge telephones

The production supervisor in Houston selects the less expensive company tie line to call the manager at the Administration office in Dallas. Once the line is selected, the production supervisor dials the digits that will map onto the target line of the manager in Dallas.

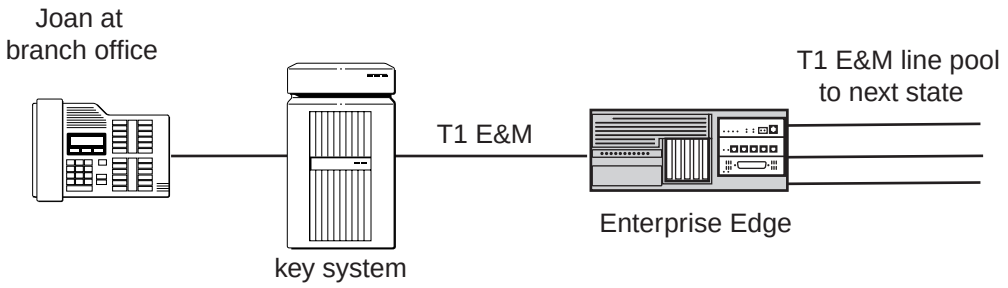


Hardware: Enterprise Edge, an EE-DTM with a T1 E&M line.

Heading	Parameter	Setting
Incoming trunk: Trunk/Line Data	 Received # Line 061 Answer Mode	 4321(for target line 243) T1 E&M Auto
Rec'd # length	Received # length	4 digits (can be from 2 to 7 digits, but must match number of digits sent by central office)

Call Enterprise Edge and select tie lines to other nodes in the private network

At a branch office, Joan selects a tie line to the main office downtown. After hearing the dial tone, she dials a line pool access code to select another tie line to a branch office in the next state.

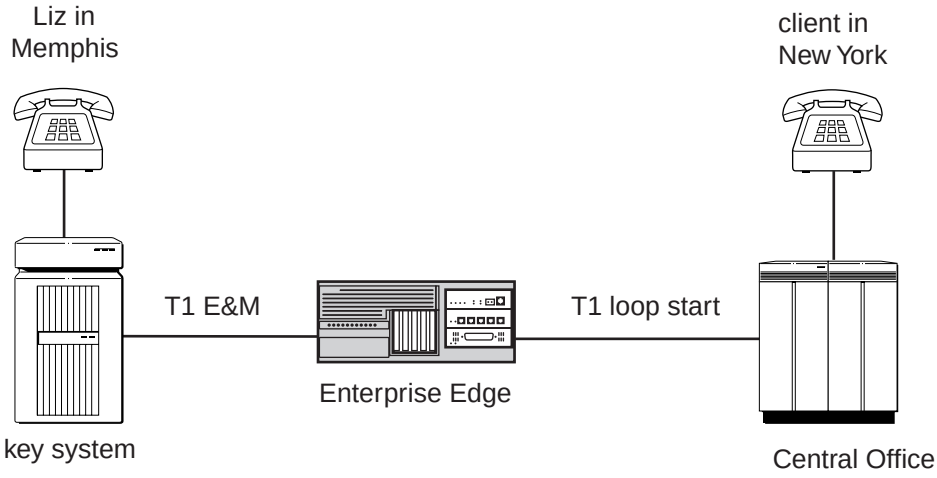


Hardware: Enterprise Edge, an EE-DTM with four T1 E&M lines (3 lines in the line pool and 1 incoming line).

Heading	Parameter	Setting
Incoming trunk: Trunk/Line Data	 Line 061 Answer mode	 T1 E&M Auto
Under Lines /Restrictions and Remote access		Define restriction filters. Define remote access packages. Assign a remote restriction and remote package to the trunk.
Outgoing trunk: Trunk/Line Data	 Line 062 Line type	 T1 E&M Pool D
Access codes	Line pool D	71 (can be from 1 to 4 digits)
Lines /Restrictions		Assign a restriction filter to the trunk.

Call Enterprise Edge and select lines to the public network

In Memphis, Liz needs to call long-distance to a client in New York. She selects a tie-line to the branch office in New York. After hearing the dial tone, she dials a line pool access code to select a line to the public network. Then, she dials the client's number as a local call.

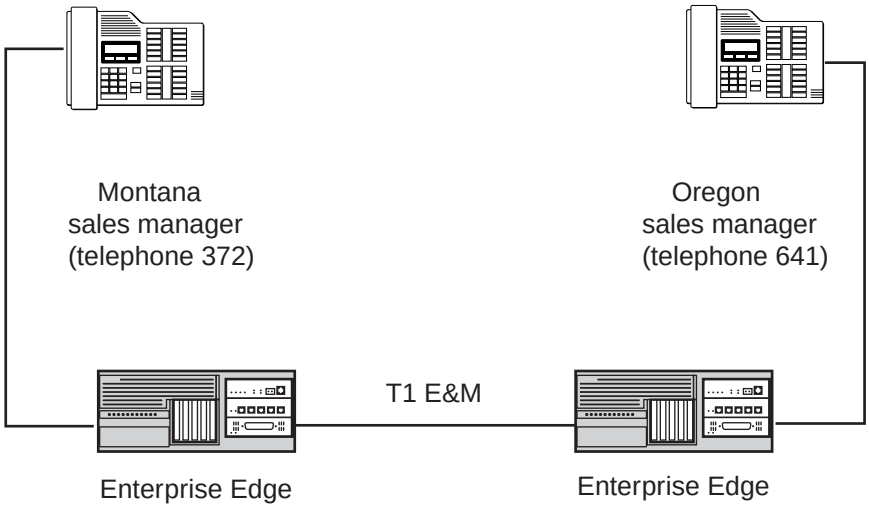


Hardware: Enterprise Edge, an EE-DTM with a T1 E&M line.

Heading	Parameter	Setting
Incoming trunk: Trunk/Line Data	Line 091 Answer mode	T1 E&M Auto
Under Lines /Restrictions and Remote access		Define restriction filters and remote access packages. Assign a remote restriction and remote package to the trunk.
Outgoing trunk: Trunk/Line Data	Line 061 Line type	Loop Pool B
Access codes	Line pool B	73 (can be 1 to 4 digits)
Lines /Restrictions		Assign a restriction filter to the line.

Select T1 E&M trunks to the private network

For a confidential call, the Montana sales manager presses the line button for a private E&M trunk to the Oregon office. This automatically alerts at the line appearance on the telephone of the Oregon sales manager.



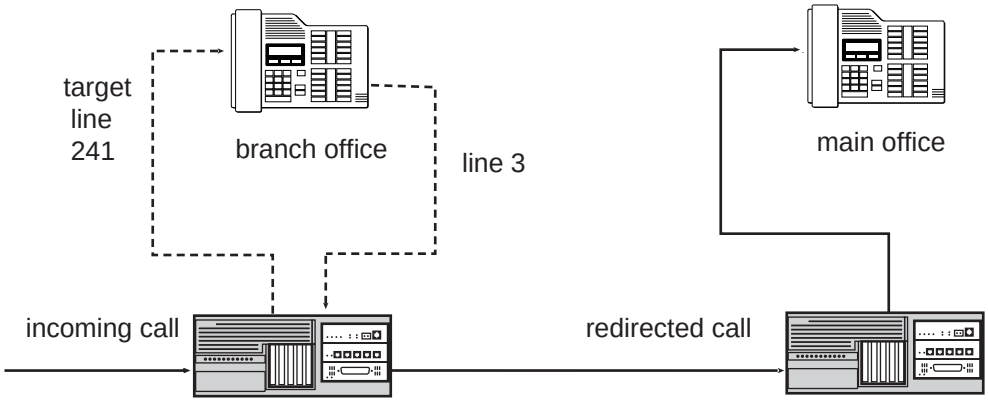
Hardware: (for both systems) Enterprise Edge, an EE-DTM with a T1 E&M line.

Heading	Parameter	Setting
Montana: *Outgoing trunk:* Trunk Data (Line 049) Line Data (Line 049)	 Line Line type	 T1 E&M Private to 372
Oregon: *Incoming trunk:* Trunk Data (Line 057)	 Line Answer mode Line type	 T1 E&M Manual Private to 641

Enterprise Edge Line Redirection feature

The branch office is receiving more calls than it can handle, so it redirects one of its lines to the main office. All calls that come in on target line 241 will be routed out on line 003 to the main office. Whenever a call is redirected, the target line and outgoing line will be busy for the duration of the call.

The branch office only routes out one call at a time on the redirected line. If the target line is busy, the next incoming call will go to the prime set and not be redirected.



Hardware: Enterprise Edge, an EE-DTM with one T1 E&M line or one T1 DID line.

Tips

Any line appearance on a telephone can be selected as the incoming line to be redirected. Restriction filter restrictions on the line are checked against the filter in effect at the time a call is redirected not when redirection is programmed.

A target line can not be selected as the outgoing line for redirection. The incoming trunk must have disconnect supervision.

Heading	Parameter	Setting
Incoming trunk: Trunk/Line Data	Line 061: T1 Loop Trunk mode: Super Answer mode: Auto OR Line 065: T1 DID OR Line 065: T1 E&M Answer mode: Auto Received #: 4321 (for target line 232)	Incoming trunk: Trunk/Line Data
Rec'd # length	Received # length: 4 digits (can be from 2 to 7 digits, but must match number of digits sent by central office)	Rec'd # length
Outgoing trunk: Trunk/Line Data	Line 062: T1 Loop OR Line 066: T1 E&M	Outgoing trunk: Trunk/Line Data
Capabilities	Allow redirect: Y	Capabilities

PRI dialing plan example for 2-way DID

The following list shows the steps involved in configuring a dialing plan for two-way DID using a Public service. In this example the user dials the prefix 8 to place a call over a PRI line.

- in the Unified Manager under **Hardware**, configure the DTI (EE-DTM) for PRI
- select **Public** as the protocol
- for incoming calls you need to program target lines to match the DID digit that is being received on the PRI interface
- set **Dial Out** to **None**
- select **PRI-A** as the line pool
- set **ServiceType** to **Public**
- under **Services, Routing Service** enter a Destination Code (8 in this example)
- set **Absorb Length** to **All**
- the set that you are dialing out from must have access to the PRI Pool (programmed in **Terminals & Sets**)
- define received digits for target lines
- define limits for incoming and outgoing public calls, see Programming Call by Call service selection on page 154.

Note: 2-way DID does not have to be configured for Call-by-call service.

PRI DID and 2-way DID

When configuring PRI DID with 2-way service, the channels programmed as DID at the CO must be the lowest B-channels on PRI. On your Enterprise Edge system, the BchanSeq mode must be set to **descending**. In this configuration, all calls on PRI must be Public service.

For example, channels 1 to 4 are configured as DID at the CO. The CO uses **ascending** mode for B-channel selection, and Enterprise Edge uses **descending** mode.

Appendix B: ISDN Overview

Welcome to ISDN

This chapter provides you with some background information about ISDN and also includes information about:

- Analog vs. ISDN
- Type of ISDN service
- ISDN layers
- ISDN Bearer capability
- Services and features for ISDN PRI
- ISDN hardware
- ISDN standards compatibility

Integrated Services Digital Network (ISDN) technology provides a fast, accurate and reliable means of sending and receiving voice, data, images, text, and other information through the telecom network.

ISDN uses existing analog telephone wires and divides it into separate digital channels which dramatically increases the bandwidth.

ISDN uses a single transport to carry multiple information types. What once required separate networks for voice, data, images, or video conferencing is now combined onto one common high-speed transport.

Nortel endeavours to test all variations of ISDN PRI on Enterprise Edge; however, due to the number of variations, this is not always possible.

Analog versus ISDN

ISDN offers significantly higher bandwidth and speed than analog transmission because of its end-to-end digital connectivity on all transmission circuits. Being digital allows ISDN lines to provide better quality signaling than analog POTS lines, and ISDN out-of band data channel signaling offers faster call set up and tear down.

While an analog line carries only a single transmission at a time, an ISDN line can carry one or more voice, data, fax, and video transmissions simultaneously.

An analog modem operating at 14.4 K takes about 4.5 minutes to transfer a 1MB data file and a 28.8K modem takes about half that time. Using one channel of an ISDN line, the transfer time is reduced to only 1 minute and if two ISDN channels are used, transfer time is just 30 seconds.

When transmitting data, the connect time for an average ISDN call is about 3 seconds per call, compared to about 21 seconds for the average analog modem call.

ISDN PRI channels

With primary rate interface (PRI), each line is made up of separate channels known as B and D channels which transmit information simultaneously.

- PRI is known as “23B+D” because it consists of 23 B-channels and 1 D-channel.

B channels

B channels are the bearer channel and are used to carry voice or data information and have speeds of 64 kbps. Since each ISDN line has more than one B-channel, a user can perform more than one transmission at the same time using a single ISDN line.

D channels

The standard signaling protocol is transmitted over a dedicated data channel called the D-channel. The D-channel carries call setup and feature activation information to the destination and has speeds of 64 kbps PRI. Data information consists of control and signal information and packet-switched data such as credit card verification.

ISDN layers

ISDN layers refer to the standards established to guide the manufacturers of ISDN equipment and are based on the OSI (Open Systems Interconnection) model. The layers include both physical connections, such as wiring, and logical connections, which are programmed in computer software.

When equipment is designed to the ISDN standard for one of the layers, it works with equipment for the layers above and below it. There are three layers at work in ISDN for Enterprise Edge. To support ISDN service, all three layers must be working properly.

- Layer 1: A physical connection that supports fundamental signaling passed between the ISDN network (your service provider) and the Enterprise Edge system.
- Layer 2: A logical connection between the central office or the far end and the Enterprise Edge system. Without Layer 2, call processing is not possible and there is no dial tone.
- Layer 3: Also a logical connection between the ISDN network (your service provider) and the Enterprise Edge system. This controls which central office services are available to the connection. For example, a network connection can be programmed to carry data calls.

The system of layers is important when you are installing, maintaining, and troubleshooting an ISDN system.

ISDN Bearer capability

Bearer capability describes the transmission standard used by the PRI line so that it can work within a larger ISDN hardware and software network.

The bearer capability for PRI is voice/speech, 3.1 kHz audio, and data (unrestricted 64 kbps, restricted 64 kbps, or 56 kbps).

Services and features for ISDN PRI

As part of an ISDN digital network, your system supports enhanced capabilities and features, including:

- faster call set up and tear down
- high quality voice transmission
- dial-up Internet and local area network (LAN) access
- video transmission
- network name display
- name and number blocking
- access to public protocols
- Call by Call service selection
- coordinated dialing plan
- Emergency 911 dialing, internal extension number transmission
- access to Meridian 1 private networking SL-1 protocol (premium telephony)

Network name display

This feature allows ISDN to deliver the Name information of the users to those who are involved in a call that is on a public or private network.

Your Enterprise Edge system displays the name of an incoming call when it is available from the service provider. If the Calling Party Name has the status of “private” it may be displayed as “Private name” if that is how the service provider has indicated that it should be displayed. If the Calling Party Name is unavailable it may be displayed as “Unknown name”.

Your system might display the name of the called party on an outgoing call, if it is provided by your service provider. Your system sends the Business Name concatenated with the set name on an outgoing call but only after the Business Name has been programmed.

The available features include:

- Receiving Connected Name
- Receiving Calling Name
- Receiving Redirected Name
- Sending Connected Name
- Sending Calling Party Name

Network Name Display on page 149 Consult your customer service representative to determine which of these features is compatible with your service provider.

Name and number blocking

When activated, Feature 8 1 9 allows you to block the outgoing name and/or number on a per-call basis. Name and number blocking can be used with an Enterprise Edge set.

Consult your customer service representative to determine whether or not this feature is compatible with your provider.

Call by Call service selection for PRI

PRI lines can be dynamically allocated to different service types with the Call by Call feature. PRI lines do not have to be pre-allocated to a given service type. Outgoing calls are routed through a dedicated PRI Pool and the calls can be routed based on various schedules.

The service types that may be available, depending on your service provider are described below.

Public

Public service calls connect your Enterprise Edge set with a Central Office (CO). DID and DOD calls are supported.

Private

Private service calls connect your Enterprise Edge set with a Virtual Private Network. DID and DOD calls are supported. A private dialing plan may be used.

Tie

Tie services are private incoming and outgoing services that connect Private Branch Exchanges (PBX) such as Enterprise Edge.

FX (Foreign Exchange)

FX service calls logically connect your Enterprise Edge set to a remote CO. It provides the equivalent of local service at the distant exchange.

Outwats

Outwats is for outgoing calls. This allows you to originate calls to telephones in a specific geographical area called a zone or band. Typically a flat monthly fee is charged for this service.

Inwats

Inwats is a type of long distance service which allows you to receive calls originating within specified areas without a charge to the caller. A toll-free number is assigned to allow for reversed billing.

Consult your customer service representative to determine whether or not this feature is compatible with your provider.

Emergency 911 dialing

The ISDN PRI feature is capable of transmitting the telephone number and internal extension number of a calling station dialing 911 to the Public Switched Telephone Network. State and local requirements for support of Emergency 911 dialing service by Customer Premises Equipment vary. Consult your local telecommunications service provider regarding compliance with applicable laws and regulations. For most installations the following configuration rules should be followed, unless local regulations require a modification.

- All PSTN connections must be over PRI
- In order for all sets to be reached from a Public Safety Answering Position (PSAP), the system must be configured for DID access to all sets. In order to reduce confusion, the dial digits for each set should be configured to correspond to the set's extension number
- The OLI digits for each set should be identical to the DID dialed digits for the set
- The routing table should route "911" to a PRI line pool
- If attendant notification is required, the routing table must be set up for all 911 calls to use a dedicated line which has an appearance on the attendant's console
- The actual digit string "911" is not hard-coded into the system. More than one emergency number can be supported

If transmission of internal extension numbers is not required or desired, then it is recommended that the person in charge of the system maintain a site map or location directory that allows emergency personnel to rapidly locate an Enterprise Edge set given its DID number. This list should be kept up to date and readily available.

2-way DID

With PRI the same lines can be used for receiving direct inward dialing (DID) and for making direct outward dialing (DOD) calls.

The dialing plan configured by your customer service representative determines how calls are routed. Consult your customer service representative to determine whether or not this feature is compatible with your service provider.

Dialing Plan and PRI

The Dialing Plan supports PRI connectivity to public and private networks. The dialing plan is a collection of features responsible for processing and routing incoming and outgoing calls. All PRI calls must go through a dialing plan.

The Dialing Plan

- allows incoming calls to be routed to sets based on service type and digits received
- provides the ability to map user-dialed digits to a service type on a Call by Call basis
- allows long distance carrier selection through user-dialed Carrier Access Codes

Consult your customer service representative to determine how your dialing plan is configured.

ISDN hardware

The Digital Trunk Media Bay Module (EE-DTM) is configured for PRI. The EE-DTM is also referred to as the Digital Trunk Interface (DTI). In most PRI network configurations, you need one EE-DTM configured as PRI to act as the primary clock reference. The only time when you may not have an EE-DTM designated as the PRI primary clock reference is in a network where your Enterprise Edge system is connected back-to-back with another switch using a PRI link. If the other switch is loop-timed to your Enterprise Edge system, your EE-DTM (PRI) can be designated as a timing master.

If your Enterprise Edge has two EE-DTMs configured as PRI, you must assign one EE-DTM as the primary reference and one as the secondary reference.

Clock Source for ISDN

Systems with ISDN interfaces need to synchronize clocking with the ISDN network. Systems synchronize clocking to the first functionally available network connection. If there are excessive errors on the reference network connection, the next available network connection is used for clock synchronization. The clock synchronization process generates alarm codes and event messages.

ISDN standards compatibility

Enterprise Edge ISDN equipment supports National ISDN standards for basic call and calling line identification services.

Enterprise Edge PRI is compliant with National ISDN-2.

Enterprise Edge does not support EKTS (Electronic Key Telephone System), CACH (Call Appearance Call Handling), or Calling Name Display.

Ordering ISDN PRI service in Canada

In Canada, order Megalink™ service, the trade name for standard PRI service and set the Enterprise Edge equipment to the supported protocol that is identified by your service provider, either DMS-100 or NI-2.

Ordering ISDN PRI service in United States

In the United States order PRI service from your service provider. Set the Enterprise Edge equipment to the PRI protocol indicated by your service provider.

Supported ISDN protocols

The switch used by your service provider must be running the appropriate protocol software and the correct version of that software to support ISDN PRI. Each protocol is different and supports different services. Contact your service provider to make sure that your ISDN connection has the protocol you require.

For more information on the supported protocols and services, refer to Call by Call service selection for PRI on page 151.

ISDN programming

Most of the programming for PRI is done under Hardware.

PRI programming activity	Programming heading
View or change the Digital Trunk Media Bay Module (EE-DTM), also referred to as the Digital Trunk Interface (DTI) Configure EE-DTM for PRI	Hardware, Modules
Provision or pre-provision lines	Maintenance, Provisioning
Enable or disable EE-DTM	Maintenance, Module status
View status of line	Maintenance, Module/port status

Program PRI resources

Some steps will not be necessary depending on the service you are using. More detailed information is included under the individual headings and settings in the **System Programming** and **Maintenance** sections of the Unified Manager. For complete module installation instructions and safety precautions, see the *Enterprise Edge Installation and Maintenance Manual*.

1. Collect the information supplied by your service provider to support your ISDN package.

2. Install the EE-DTM.

3. Disable each module under Maintenance.

4. Configure the EE-DTM for PRI in Hardware and provision the module.

5. Re-enable the module in Maintenance. If required, the module goes through a firmware download process, which takes five to six minutes.

Program PRI lines

When the configuration programming under Hardware is complete, your PRI lines are ready to be programmed. For information on programming your PRI lines, see Call by Call service selection for PRI on page 151.

Program Direct Inward System Access (DISA) on PRI lines

When an EE-DTM is configured for PRI, all lines on that module are set to Auto Answer without Direct Inward System Access (DISA). DISA can however be accessed by one of two methods.

1. Define the DISA DN to match the trailing digits of the Called Party Number (CDN).

   With Public, Private, and Tie service types, the CDN is simply truncated to the Target Line Receive Digit Length and is parsed to match the Target Line Receive Digits. DISA can be accessed by having the DISA DN match the trailing digits of the CDN. For example, with a Receive Digit Length = 4, and DISA DN = 1234, a call made to Public DN 763-1234 will be handled as follows:

   - the ISDN setup message will contain a CDN of 763-1234
   - the CDN will be truncated to the 4 digits, 1234
   - 1234 matches the DISA DN
   - the call will be answered with DISA

2. Use incoming Call by Call (CbC) Service routing to map the call type to the DISA DN. Refer to Call by Call service selection for PRI on page 151 for more information.

   With FX, INWATS, 900, and SDS service types, either a Service Id (SID) or a CDN is mapped to Target Line Receive Digits. This is programmed under Call-by-Call Routing. DISA may be accessed by having the SID or CDN map to the DISA DN. This example has a Receive Digit Length = 4, DISA DN = 1234, and CbC Routing with (Service Type = FX, Map from SID = 2, Map to digits = 1234).

   A call presented to the Enterprise Edge system with service type FX and SID 2 will be handled as follows:

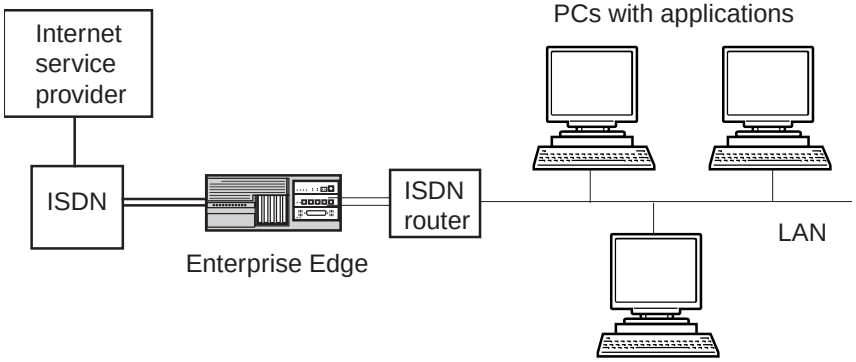
   - The ISDN setup message will specify FX with SID = 2
   - The FX SID = 2 will be mapped to DISA DN digits 1234

   The call will be answered with DISA

Program ISDN equipment

ISDN router

By connecting an ISDN router to your Enterprise Edge system, a group of PCs can share Internet access. This arrangement is best for a workplace where each PC uses an Internet connection.



To support Internet access, you must order PRI lines from your service provider, and subscribe to Internet service from an Internet service provider (ISP). Your PCs must have an Internet browser and any applications supplied by your ISP.

Appendix C: Setting Up Remote Routers

This appendix includes information on setting up Nortel Networks (BayRS) routers and how to set up a range of UDP as a high priority.

This chapter includes:

- Creating an Outbound Traffic Filter
- Sample Criteria, Ranges, and Actions for UDP Filtering

Creating an Outbound Traffic Filter

To create an outbound traffic filter:

1. In the Configuration Manager window, click **Circuits** and then click **Edit Circuits**.
   The Circuit List window appears.

2. Select a circuit.

3. Click the **Edit** button.
   The Circuit Definition screen appears with the circuit you selected highlighted.

4. Click **Protocols**, click **Edit Protocol Priority,** and then click **Priority/Outbound Filters**.
   The Priority/Outbound Filters window appears.

5. Click **Template**.
   The Filter Template Management window appears.

6. Click **Create**.
   The Create Priority/Outbound Template window appears.

7. Enter a descriptive name in the Filter Name field.

8. Click **Criteria**, click **Add**, click **Datalink**, click **IP,** and then click **Criterion**.
   The Add Range window appears. If you choose the User-Defined criterion, the Add User-Defined Field window appears first.

9. Type a minimum and maximum value to specify the range and click the **OK** button.
   The Add Range window closes. The new criterion and ranges now appear in the Filter Information field of the Create Priority/Outbound Template window.

10. Click **Action**, click **Add** and then click ***action***.

11. Click the **OK** button.
    The Filter Template Management window opens. The new template appears in the templates list.

12. Click **Done**.
    The Priority/Outbound Filters window opens.

13. Click **Create**.
    The Create Filter window opens.

14. Select a circuit in the Interfaces field.

15. Select a template in the Templates field.

16. Enter a descriptive name in the Filter Name field.

17. Click **OK**.
    The Priority/Outbound Filters window opens.

18. Click **Apply**.
    The filter is applied to the circuit.

Sample Criteria, Ranges, and Actions for UDP Filtering

The filtering goal is to place all VoIP H.323 traffic leaving a particular interface in the high priority queue. From the BayRS Site Manager:

Use a criteria path of **Criteria**, **Add**, **IP**, **IP**, **UDP Destination Port**

The range is 2065 to 2067.

The action path is: **Action**, **IP**, **Add**, **High Queue**.

Note: This example shows how to give H.323 traffic priority over other protocols on the interface.

Glossary

A

AbsorbLength

A setting that determines how many of the digits in a destination code will not be dialed by the system. AbsorbLength is assigned under Destination codes in Services.

access code

Different sequences of characters used to gain access to the features: Line pools, Call park, external lines, Direct-Dial telephone and Auto DN.

address

A unique identifier assigned to networks and stations that allows each device to receive and reply to messages.

Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a physical machine address that is recognized in the local network. For example, in IP Version 4, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. The physical machine address is also known as a Media Access Control or MAC address. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

alarm code

A number that is displayed, informing you that a fault has been detected in the system.

Analog Terminal Adapter

A device that permits the connection of analog telecommunication devices such as fax machines, answering machines, and single line telephones to the Enterprise Edge system.

ANSI

American National Standards Institute.

Answer button

A telephone button with an indicator that is used to monitor another telephone. The answer button indicates incoming calls destined for the other telephone. Someone working at a telephone with answer buttons (an attendant, for example) can receive all ringing and visual indication of incoming calls for other telephones, and answer those calls when necessary.

One telephone can have up to four Answer buttons. An Answer button is automatically assigned to a telephone when that telephone is assigned an Answer DN.

Answer DN

The internal or directory number (DN) of a telephone that is monitored by an Answer button. You can assign up to four Answer DNs to a telephone under Line Access in Terminals and Sets programming.

Application Program Interface (API)

An API is the specific method prescribed by an operating system or by another application program when a programmer writes an application program. The API is used to make requests of the operating system or another application.

Unlike the graphical user interface or command interface, which are direct user interfaces, the API is an interface to an operating system or a program.

Application

A computer program that performs a wide range of tasks as specified by the user. Examples of application programs include word processing packages, spreadsheet packages and accounting packages.

ARP

See Address Resolution Protocol.

asynchronous

A method of transmission where the time intervals between characters are not required to be equal and signals are sourced from independent clocks with different frequencies and phase relationships. Start and stop bits may be added to coordinate character transfer.

Autobumping

A feature that determines what the system does with new Call Log items when your Call Log is full. When Autobumping is on, a new log entry causes the oldest entry to be deleted. If Autobumping is off, your system does not log calls when your log is full.

autodial button

A memory button that, if programmed, provides one-touch dialing of external or internal numbers.

autolog options

A feature that allows you to select the type of calls that are stored in your Call Log. You can choose to log calls that were not answered by anyone within the system, to log calls that were unanswered at this telephone but answered elsewhere in the system, to log all calls answered and not answered at this telephone, or to not have calls automatically logged.

Automatic Dial

A feature that allows you to dial without having to pick up the receiver or select a line. You must have a prime line to use Automatic Dial. Automatic Dial is assigned under Dialing options in Terminals and Sets programming.

Automatic Handsfree

A feature which automatically activates Handsfree operation when you make or answer a call. Automatic Handsfree is assigned under Handsfree in Terminals and Sets programming.

Automatic Hold

A feature that automatically places an active call on hold when you select another line. Automatic Hold (Full AutoHold) is assigned in Lines programming.

Automatic Privacy

See Privacy.

Automatic Daylight Savings Time

A feature that switches the system to standard or daylight savings time at pre-programmed times. It is turned on or off under Daylight time in System programming.

Automatic Telephone Relocation

A feature that lets a telephone retain its personal and system programming when it is plugged into a different modular jack. Automatic Telephone Relocation is enabled under Set relocation in System programming.

auxiliary ringer

A separate external telephone ringer or bell which can be programmed to ring when a line or a telephone rings. An auxiliary ringer may be programmed to ring only when the system is in a particular schedule. Programming of an auxiliary ringer is done in Services programming after the feature has been enabled under Capabilities in Terminals and Sets programming.

AWG

American wire gauge.

B

B channel (Bearer channel):

An ISDN standard transmission channel used for voice or data transmission.

Background Music:

A feature that lets you hear music from the speaker of your telephone. It is available only if a music source has been attached to the system and the feature has been enabled under Feature settings in System programming.

Back up

To make a duplicate copy of data files so that you can store the originals in a safe place. Backing up your original files protects them from damage if a hardware failure occurs.

Base Station:

A Companion component that is mounted on walls and ceilings to provide a radio link to an office or other area where Companion portable telephones are used. Each Base Station houses two radios that allow portables to send and receive calls through the Enterprise Edge Server.

Baud rate

A unit of measurement of data transmission speed. It is approximately equivalent to Bits Per Second (BPS). Typical baud rates are 300, 1200, 2400, 4800, and 9600.

Bearer channel:

See B channel.

BERT:

See bit error rate test.

BIOS (Basic Input Output System)

A program contained in Read Only Memory (ROM) that acts as the interface between software programs and the computer hardware.

Bit

An abbreviation for Binary Digit. A bit is the smallest unit of information recognized by the computer. A bit has one of two values (0 or 1) to indicate off or on.

bit error rate test:

A test that checks the transmission of data across the voice and data channels between the system and any telephone.

BPS (Bits Per Second)

The speed of data transmission between two computers.

Basic Rate Interace (BRI)

An ISDN interface which uses two B channels and a D channel (2B+D).

Bus

A collection of communication lines that carry electronic signals either between elements on the system board or between the circuitry on the system board and any cards plugged into the system board.

busy lamp field (BLF):

A device with a liquid crystal display (LCD) panel of indicators that shows the status of up to 24 telephones in the system.

Byte

The amount of space required to store a single character. One byte equals eight bits.

C

Call Duration timer

A feature that lets you see how long you spent on your last call or how long you have been on your present call.

Call Forward

A feature that forwards all the calls arriving at your telephone to another telephone in your system. To have calls forwarded outside the system, use Line Redirection.

Call Forward No Answer

A feature that forwards all calls arriving at your telephone to another designated telephone in your system after a specific number of rings. Call Forward No Answer is assigned under Capabilities in Terminals and Sets programming.

Call Forward On Busy

A feature that forwards all calls at your telephone to another designated telephone if your telephone is busy. This feature is assigned under Capabilities in Terminals and Sets programming.

Call Forward Override

An automatic system feature that lets you call someone and ask them to stop forwarding their calls to you.

Call Information

Call Information allows you to display information about incoming calls. For external calls, you can display the caller's name, telephone number and the line name. For an internal call, you can display the name of the caller and their internal number. You can obtain information about ringing, answered, or held calls.

Call Log

Enter your Call Log to view a record of incoming calls. The log could contain the following information for each call: sequence number in the Call Log, name and number of caller, long distance indication, indication if the call was answered, time and date of the call, number of repeated calls from the same source, and name of the line that the call came in on. See Autobumping, Autolog options, and Call Log for further information.

Call Park

With this feature you can place a call on hold so that someone can retrieve it from any other telephone in the system by selecting an internal line and entering a retrieval code.

The retrieval code appears on the display of your telephone when you park the call. You can park up to twenty-five calls on the system at one time.

Call Park Callback

See Callback.

Call Park prefix

The first digit of the retrieval code of a parked call. This digit cannot conflict with the first digit of any existing DNs, Line Pool access codes, the Direct-dial digit, or the external line access code. The default Call Park prefix digit is “1”. It may be set to none, in which case Call Park is disabled. Call Park prefix is assigned under Access codes in System programming.

Call Pickup Directed

A feature that lets you answer a call ringing at any telephone by entering the internal number of that telephone before taking the call. Call Pickup Directed is enabled under Feature settings in System programming.

Call Pickup Group

See Pickup Group.

Call Queuing

If you have several calls waiting at your telephone, you can invoke the Call Queuing feature to answer them in order of priority. Priority is given to incoming calls, followed by callback and camped calls.

Callback

If you park, camp, or transfer a call to another telephone and it is not answered there, it will ring again at your telephone. How long the system will wait before Callback occurs is set under Feature settings in System programming.

Camp-on

A feature that lets you reroute a call to a telephone even if all the lines on that telephone are busy. To answer a camped call, use Call Queuing or select a line if the camped call appears on your telephone. Priority is given to queued calls over camped calls.

Camp timeout

The length of a delay before a camped call is returned to the telephone that camped the call. The length of delay is set under Feature settings in System programming.

Central answering position (CAP)

An M7324 telephone that has been designated as a CAP under CAP assignment in System programming. The CAP provides backup answering and can be used to monitor the telephones within a system.

Central answering position (CAP) module

A module connected to an M7324 telephone and provides 48 additional buttons that can be used as autodial buttons or feature buttons. A maximum of two CAP modules can be connected to a single M7324 telephone.

Channel Service Unit (CSU)

A device on the Digital Trunk Interface that is the termination point of the T1 lines from the T1 provider. The CSU collects statistics on the quality of the T1 signal. The CSU ensures network compliance with FCC rules and protects the network from harmful signals or voltages.

Challenge-Handshake Authentication Protocol (CHAP)

CHAP is a method of establishing security on PPP links where the peers must share a plain text identifier. The caller sends a challenge message to its receiving peer and the receiver responds with a value it calculates based on the identifier. The first peer then matches the response with its own calculation. If the values match, the link is established.

CHAP is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP).

Class of Service (COS)

The set of features and lines available to the user for a call. The Class of Service for a call is determined by the restriction filters and remote access packages assigned to the telephone in Lines programming. The Class of Service for a call can be changed by entering a six-digit Class of Service password. (Internal users cannot change their access to features with a COS password, only their restriction filters.) Class of Service and Class of Service passwords are assigned in Passwords programming. See Remote Access.

Class of Service password

A six digit code that lets you switch from your current Class of Service to one that lets you dial numbers prohibited by your current Class of Service.

client

A client is a computer system or process that requests a service of another computer system or process. A workstation requesting the contents of a file from a file server is a client of the file server.

cold start

A cold start occurs when all system programming is lost. This can happen after a major event such as an extended power failure.

Companion Wireless

The name for the communication systems which use radio technology to transmit and receive signals between its components and the Enterprise Edge Server. Companion Wireless provides mobility in the workplace. Calls that used to ring just at your telephone set can also appear and ring at your portable.

Companion portable telephone

Hand-held wireless telephones that allow complete mobility within the reach of Companion Base Stations or an external antenna. Portables offer many but not all standard system features and share much of the same programming as “wired” desk telephones.

Conference

A feature that allows you to establish a three-person call at your telephone.

Conventions

The way certain information is described. For example, using underlined text to represent second-line display prompt information.

COS

See Class of Service.

D

D channel (Data channel)

An ISDN standard transmission channel which is packet-switched, and is used for call setup, signalling and data transmission.

Data channel

See D channel.

Data link connection indentifier (DLCI)

The DLCI is used to identify a PVC in frame relay networks.

Defaults

The settings for all features when the system is first installed. Settings are changed from their defaults in programming.

Delayed Ring Transfer (DRT) to prime

After a specified number of rings, this feature transfers an unanswered call on an external line to the prime telephone associated with that line. This feature is activated under Feature settings in System programming.

destination code

A two- to seven-digit number that the system interprets and then translates into the digits that you want dialed out. Both the code and its associated dialed digits are assigned under Routing service in Services programming.

DHCP

See Dynamic Host Configuration Protocol.

dialing restriction

See Restriction filter.

dial-up connection

A dial-up connection is a temporary connection between computers that is established over an analog or digital phone line.

Differentiated Services (DiffServ)

DiffServ is a implementation methodology for QoS service for IP networks. DiffServ is a rule based methodology intended to improve network performance. Instead of applying faster, more advanced technology, networks are managed by appropriate network policies. With DiffServ there is a cost associated with higher quality services and a risk with lower quality services.

Direct-dial

A feature that lets you dial a designated telephone in your system with a single digit. As many as five direct dial sets can be established. Each telephone in the system is assigned to one direct-dial telephone. There is a single, system wide digit for calling the assigned direct-dial telephone of any telephone. Direct-dial telephones are established in System programming. Telephones are assigned to a direct-dial telephone under Capabilities in Terminals and Sets programming.

Direct-dial

A digit used system-wide to call the Direct-dial telephone. The digit is assigned under Access codes in System programming.

Direct-dial number

The digit used to call the direct-dial telephone.

directed pickup

See Call Pickup Directed.

Directory number (DN)

A unique number that is automatically assigned to each telephone or data terminal. The DN, also referred to as an internal number, is often used to identify a telephone when settings are assigned during programming.

Disconnect Supervision

A setting that enables the system to detect if an external caller hangs up. Once an external caller hangs up, the system can disconnect its line. Disconnect Supervision is enabled under Trunk/Line data in Lines programming.

Disk drive

A mass storage device that seeks, reads and writes data on a disk.

Display

A one-line or two-line screen on an Enterprise Edge telephone that shows commands and options.

Display buttons

The three buttons that appear underneath an Enterprise Edge two-line LCD display.

Display options

The choices available to a user that appear on the Enterprise Edge two-line display. Options appearing on the display can be selected using the display or dialpad buttons.

DLCI

See Data link connection indentifier.

DN

See Directory number.

DNS

See Domain Name Server.

domain name

The domain name is used to organize Internet names into manageable groups, such as nortelnetworks.com.

Domain Name Server (DNS)

The domain name system or domain name server is the system in the Internet that maps names of objects, most usually host names, into IP numbers or other resource record values. The namespace of the Internet is divided into domains, and the responsibility for managing names within each domain is delegated, typically to systems within each domain.

Do Not Disturb

A feature that stops calls from ringing at your telephone. Only Priority Calls will ring at your telephone. A line button will flash when you receive a call, but the call will not ring.

Driver (Device)

A program that allows a hardware peripheral, such as a NIC, to communicate with the Enterprise Edge Server.

DTMF

See Dual tone multifrequency.

dual tone multifrequency

Two distinct telephone signaling tones used for dialing.

Dynamic Host Configuration Protocol (DHCP)

DHCP is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses in an organization's network. Using the Internet's set of protocols (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine.

Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

E

Emergency 911 dialing

The capability to access a public emergency response system by dialing the digits 9-1-1. State and local requirements for support of Emergency 911 Dialing service by Customer Premises Equipment vary. Consult your local telecommunications service provider regarding compliance with applicable laws and regulations.

emergency telephone

A single-line telephone (also referred to as a 500/2500 telephone) that becomes active when there is no power to the Enterprise Edge Server.

Ethernet

A widely used Local Area Network (LAN) protocol that is the original Carrier Sense Multiple Access/Collision Detect (CSMA/CD) LAN that lets PCs and/or Enterprise Edge Servers listen for pauses before they communicate. Ethernet LANs use coaxial cable or twisted pair wiring for connecting computers.

evening schedule

See Schedules and Services.

event message

Event messages are stored in the system log and displayed during a Maintenance session. They record a variety of events and activities in the system.

exceptions

See Overrides.

Extended Data-Out (EDO)

Extended Data-Out (EDO) is a form of Dynamic Random Access Memory (RAM) in which storing data to and reading data from the memory is performed at a faster rate.

external call

A call to a destination outside the system.

external code

The number you dial to get an external line. By default it is 9, but this can be changed under Access codes in System programming. You do not always need an external code. It is primarily to support the M7100 telephone and single line telephones using an Analog Terminal Adapter.

external line

A line on your telephone used for making calls to destinations outside the system.

external music source

See Music source.

external paging

A feature you can use to make voice announcements over an externally-mounted loudspeaker connected to the Enterprise Edge Server. The external speaker is not an Enterprise Edge component and must be supplied by the customer.

F

FAX

FAX works with Enterprise Edge Voice Messaging, offering a caller the capability of sending a fax document to a mailbox as easily as sending a voice message.

Feature Code

A unique code used to access Enterprise Edge features and options.

File

A collection of related information stored on a disk under a given name for later reference and used by an operating system or application program. Each application program that you use saves the data you create in files. Files are identified by a file name and optional extension.

File name

A name that identifies a file and consists of one to eight characters.

filtering

Filtering is the process of examining a data packet on the network to determine the destination of the data and whether the packet should be passed along on the local LAN, copied to another LAN, or dropped.

Forward

See Call Forward.

frame

A frame is a unit of data transmission in a local area network.

frame relay

A frame relay is a high-speed, packet switching WAN protocol designed to provide efficient, high-speed frame or packet transmission with minimum delay. Frame relay uses minimal error detection and relies on higher level protocols for error control.

FTP

The file transfer protocol (FTP) allows a user on one host to access and transfer files to and from another host over a network. On the Internet, FTP refers to a tool for accessing linked files.

Full Autohold (on idle line)

When this feature is on, if you select an available line, and then do something that selects another line, the first line is put on hold. Full Autohold is enabled under Trunk/Line data in Lines programming.

Full Handsfree

See Handsfree.

Fully Qualified Domain Name (FQDN)

The combination of host name and domain name. For example mycomputer.nortelnetworks.com is Fully Qualified Domain Name.

G

Ground Start trunk

Ground start trunks offer the same features as loop start trunks, but are used when the local service provider does not support disconnect supervision for the digital loop start trunks. By configuring lines as ground start, the system will be able to recognize when a call is released at the far end. Ground start trunks are provided only by a Digital Trunk Interface (DTI).

Group Listening

A feature that allows you to have others in your office hear a caller through your telephone speaker. The caller hears you only when you speak into the receiver and cannot hear other people in the office.

You can cancel Group Listen for the current call. Group Listen is cancelled automatically when you hang up the Group Listen call.

H

H.323

H.323 is the standard for using IP to send voice and video within intranets and on the public Internet.

Handsfree

A feature you can use to make calls without using the telephone receiver. Full Handsfree is activated under Capabilities in Terminals and Sets programming. When it is activated, a Handsfree/Mute button is automatically assigned to the telephone.

Handsfree (HF) Answerback

When activated, this feature automatically turns on the microphone at a telephone receiving a Voice Call so that the person receiving the call can respond without lifting the receiver. It is activated under Capabilities in Terminals and Sets programming.

Handsfree / Mute button

See Handsfree.

Hard disk drive

A data storage device that uses non-removable, rigid magnetic platters. Hard disk drives work faster and store more data than disk drives do for diskettes.

Hardware

The physical components of the Enterprise Edge system.

HDLC

See High-level Data Link Control.

Headset

A head-mounted or ear-mounted telephone receiver that is used instead of the hand-held receiver. Headsets are not Enterprise Edge system components and must be supplied by the customer.

Held (Line) Reminder

A telephone rings and displays the message **On hold: LINENAM** when an external call has been placed on hold for a certain period of time. The Held Line Reminder feature and Remind delay are set under Ftr settings in System programming.

HF Answerback

See Handsfree Answerback.

High-level Data Link Control (HDLC)

HDLC is a group of protocols or rules for transmitting data between network points or nodes. Data is organized into a unit, called a frame, and sent across a network to a destination that verifies its successful arrival. The HDLC protocol also manages the flow or pacing at which data is sent. HDLC is one of the most commonly-used protocols in Layer 2 of the industry communication reference model, Open Systems Interconnection (OSI).

Hold button

This button is used to suspend calls so that the person using the telephone can perform another task without disconnecting the caller.

Hook Switch Flash

See Link time.

Host Name

In networking, the name of a computer that primarily provides services, such as database access, to other computers or Enterprise Edge Servers in the domain. The host name is associated with a unique IP address. Since the Enterprise Edge Server has a unique IP address, it qualifies as a host.

Host system signaling

Also referred to as end-to-end signaling. Telephones can access a remote system or dial a number on an alternate carrier by means of host feature activation, such as Link, Pause and Run/Stop.

Hotline

This feature automatically calls a pre-assigned number when the telephone's receiver is lifted or the Handsfree/Mute button is pressed. A Hotline number can be an internal or external number. Hotline is assigned under Capabilities in Terminals and Sets programming.

HTTP

The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the world wide web.

HTTP proxy

See Web proxy.

Hz (hertz)

A unit of measure for indicating frequency in cycles per second.

I

ICMP

ICMP is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses IP datagrams, however the messages are processed by the TCP/IP software and are not directly apparent to the application user.

I/C

An abbreviation of intercom.

IETF

See Internet Engineering Task Force.

In-Band

In-band is a method of device access which utilizes a network interface component within the device.

Initialization

The steps required to prepare hardware or software for operation.

Install

To set up for operation. For example, hardware is installed by attaching it to the appropriate connectors or sockets either inside or outside the Enterprise Edge Server.

Integrated Services Digital Network (ISDN)

A digital telephone service that allows for a combination voice and data connection over a single, high-speed connection. ISDN service can operate over the same copper twisted-pair telephone line as analog telephone service.

intercom button

A button that provides access to internal lines used for calls within a Enterprise Edge system and access to external lines through a line pool or external code. A telephone may be assigned zero to eight Intercom buttons. This is done under Line access in Terminals and Sets programming.

intercom keys

See Intercom button.

Interface

An information interchange path that allows communication between computer parts.

internal line

A line on your telephone dedicated to making calls to destinations inside your system. An internal line may still connect you with an external caller if you use it to access a line pool or to pick up a call using the call handling features such as Call Park or Call Pickup Directed.

internal number

A number (also referred to as a Directory Number or DN) that identifies a telephone or device.

internal user

Someone using an Enterprise Edge telephone within the system.

Internet

A global TCP/IP network linking millions of computers for communications purposes.

Internet Engineering Task Force (IETF)

The IETF is the committee that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society's Internet Architecture Board (IAB).

Internet-standard Network Management Framework

Device configuration and monitoring via SNMP.

IP

The Internet Protocol (IP) is the protocol that supports data being sent from one computer to another on the Internet. Each computer on the Internet has at least one address that uniquely identifies it from all other computers on the Internet. When you send or receive data, the message gets divided into units called packets. Each of these packets contains both the sender's Internet address and the receiver's address.

IP is a connectionless protocol, which means that there is no established connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. In the Open Systems Interconnection (OSI) communication model, IP is in layer 3, the Networking Layer.

IP address

The Internet Protocol address is a unique identifier that allows communication over the Internet to be directed to the appropriate destination. Every computer on the Internet must have a unique IP address. IP addresses are allocated by an ISP in following format: nnn.nnn.nnn.nnn, where nnn is a numeric value from 0 to 255. IP addressing might be referred to as being static (fixed) or dynamic.

IRQ (Interrupt Request)

A signal sent by a hardware device to the microprocessor requesting its immediate attention. For example, each communications port has an interrupt request line for notifying the microprocessor when data has been received or transmitted.

IRQ Conflict

Two hardware devices are vying for same IRQ. On installation of a device where an IRQ conflict occurs, the user may have to manually configure the IRQ settings to resolve the conflict.

ISDN

See integrated services digital network.

ISDN DN

A directory number (DN) used by ISDN terminal equipment connected to the system. The Enterprise Edge system uses a maximum of thirty ISDN DNs.

K

Kbyte

The abbreviation for kilobyte. A kilobyte is equal to 1024 bytes.

L

LAN

A LAN is a network of interconnected workstations sharing the resources of a single processor or server within a relatively small geographic area.

Last Number Redial

A feature that allows you to redial the last external number you dialed.

Least cost routing

See Routing service.

line

The complete path of a voice or data connection between one telephone (or other device) and another.

Lines

A programming section that lets you assign settings to each trunk and external line.

Line number

A number that identifies an external line. The total number of lines depends on the number and type of trunk media bay modules installed.

Line Pool

A group of lines used for making external calls. Line pools provide an efficient way of giving a telephone access to external lines without taking up many line buttons. A line is assigned to be part of a line pool under Trunk/Line data in Lines programming.

Line Redirection

A feature that allows you to redirect all calls on an incoming line to a destination outside the system. Once a line is redirected it cannot be answered within the system. The system may be set up to give a brief ring when a call comes in on a redirected line, under Capabilities in Terminals and Sets programming.

This feature differs from Call Forward in two ways. It redirects only external calls (not internal calls) and it redirects calls to destinations outside the system. Call forward redirects calls only to destinations inside the system. See Call Forward.

Link

If your Enterprise Edge system is connected to a Private Branch Exchange (PBX), you can use a Link signal to access special features. The Link signal can also be included as part of a longer stored sequence on an External Autodial button or in a Speed Dial code. The Link symbol uses two of the 24 spaces in a dialing sequence.

Local Area Network (LAN)

A group of computers or Enterprise Edge Servers physically connected in a manner that lets them communicate and interact with each other.

Long Tones

A feature that lets you control the length of a tone so that you can signal devices such as fax or answering machines which require tones longer than the standard 120 milliseconds.

Lunch schedule

See Schedules, and Services.

M

MAC

The Media Access Control (MAC) is a physical address that is the portion of the data-link layer in 802.x networks that controls addressing information of the packet and enables data to be sent and received across a local area network.

Maintenance

A type of programming that is used to diagnose and repair problems in the Enterprise Edge system. Maintenance requires no programmable settings.

Mailbox

A storage place for voice messages on Enterprise Edge Voice Messaging.

message

A feature that allows you to send a message to another system user. The Message feature also lets you know if you have any messages waiting and maintains a Message Waiting List to keep a record of your internal messages and your (external) voice mail messages.

MHz

The abbreviation for megahertz. This is a unit of measure indicating frequency in millions of cycles per second.

Microprocessor

A chip that is the center of all activity inside the Enterprise Edge Server. The microprocessor controls all logical and arithmetic operations for the computer and is responsible for executing program commands. It is also referred to as the Central Processing Unit (CPU).

Modem

A communications device that allows data to be exchanged between computers over telephone lines. The exchange is done by electronic processes called modulation and demodulation. The modem changes (modulates) the data into tones to send to another modem and also converts (demodulates) tones when receiving from another modem.

Move Line buttons

A feature that allows you to move external lines to different buttons on your telephone.

Multilink PPP

Multilink PPP is an extension to the PPP protocol that enables you to group a set of links into a bundle for more bandwidth. The links in the bundle can operate at different speeds. Typical links can be ISDN B channels, dial-up connections, and leased-lines.

Music source

A radio or other source of music can be connected to the system to provide music for the Music on Hold and Background Music features. A music source is not part of the Enterprise Edge system and must be supplied by the customer.

M7100 telephone

The Enterprise Edge model M7100 telephone that has a single-line display and one programmable button without an indicator.

M7208 telephone

The Enterprise Edge model M7208 telephone that has a single-line display and eight programmable buttons with indicators.

M7310 telephone

The Enterprise Edge model M7310 telephone that has a two-line display with three display buttons, 10 programmable buttons with indicators and 12 dual programmable buttons without indicators.

M7324 telephone

The Enterprise Edge model M7324 telephone that has a two-line display with three display buttons and 24 programmable buttons with indicators.

N

Names

Names can be assigned to System Speed Dial numbers, external lines, telephones, mailboxes, ACD Queues and service schedules. This is done in programming. You can use up to sixteen characters to name a System Speed Dial number, 13 characters for mailbox and ACD Queue names, and seven characters to name a telephone, line, or schedule. If a Name has not been assigned, the line number or DN will appear on the display instead of a name.

name server

A name server provides the means of translating readable host computer names into actual IP addresses so you do not have to remember long numbers in order to access other computers and destinations on the Internet. For example, DNS servers and WINS servers are name servers.

NetBIOS

The Network Basic Input/Output System (NetBIOS) is an interface and upper-level protocol developed by IBM for use with a proprietary adapter for its PC network product. NetBIOS provides a standard interface to the lower networking layers. The protocol provides higher-level programs with access to the network. Windows NT systems use NetBIOS.

Network

Two or more computers linked together electronically to share programs and exchange data. Joining computers over a network requires adding specialized hardware and software to each computer.

network device

A network device is a hardware entity characterized by its use as a communications component within a networking infrastructure.

Network DN

A number supplied by the ISDN network service provider for ISDN terminal equipment.

Network Interface Card (NIC)

An adapter card containing the hardware necessary to connect an Enterprise Edge Server to a local area network.

NIC

A network interface card (NIC) is a computer circuit board or card that is installed in a computer so that it can be connected to a network.

Personal computers and workstations on local area networks (LANs) typically contain a network interface card specifically designed for the LAN transmission technology, such as Ethernet or Token Ring. Network interface cards provide a dedicated, full-time connection to a network.

Night schedule

See Schedules, and Services.

O

On hold

A setting, programmed under Feature settings in System programming, that controls whether external callers hear music, periodic tones, or silence when they are placed on hold.

Operating system

The disk-based software that manages the operation of the Enterprise Edge Server. An operating system controls the flow of information between the computer hardware. Windows® NT is the operating system that manages the Enterprise Edge Server.

Option

An Enterprise Edge Server choice that is given to a user through display prompts.

OPX

Off premise extension.

Out-of-Band

Out-of-band is a method of device access which circumvents the network interface components within the device.

overlay

See Programming overlay.

overflow

A setting in Routing Service that allows users to decide what path an outgoing call will take if all the lines used in a particular route are in use when the call is made.

Overrides

One component of a restriction filter. Overrides are numbers you can dial even if they are forbidden by a more general restriction. See Restrictions.

P

Packet

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, GIF file, URL request, and so forth) is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into pieces of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When the packets have all arrived, they are reassembled into the original file.

A packet-switching scheme is an efficient way to handle transmissions on a connectionless network such as the Internet. An alternative scheme, circuit-switching, is used for networks allocated for voice connections. In circuit-switching, lines in the network are shared among many users as with packet-switching, but each connection requires the dedication of a particular path for the duration of the connection.

Packet and *datagram* are similar in meaning. A protocol similar to TCP, the User Datagram Protocol (UDP) uses the term datagram.

Page

A feature you can use to make announcements over the Enterprise Edge system. You can make page announcements over the telephone speakers and/or external speakers.

Page Time out

A setting that controls how long a Page Announcement can last. It can be assigned under Feature settings in System programming.

Page zone

An area in the office that receives internal page announcements independently of the rest of the office.

Each page zone is identified by a number. Telephones are assigned to page zones under Capabilities in Terminals and Sets programming.

PAP

The Password Authentication Protocol (PAP) is a procedure used by PPP servers to validate a connection request. PAP works as follows:

1. After the link is established, the requestor sends a password and an id to the server.

2. The server either validates the request and sends back an acknowledgement, terminates the connection, or offers the requestor another chance.

Passwords are sent without security and the originator can make repeated attempts to gain access. For these reasons, a server that supports CHAP will offer to use that protocol before using PAP.

Parallel port

A port that transfers data through multiple wires so that eight bits are transmitted simultaneously. Parallel ports usually use a 25-pin interface that transmits and receives data one byte at a time using a separate data line for each bit.

Park prefix

See Call park prefix.

Park timeout

The time before an unanswered parked call is routed back to the telephone that parked it. Park timeout is under Feature settings in System programming.

Password

A four-digit to eight-digit number that is entered using the dialpad. A password is used to open mailboxes or perform configuration tasks.

Pause

A feature that enters a 1.5 second delay in a dialing sequence on an external line. This is often required for signaling remote devices, such as answering machines, or when reaching through to PBX features or host systems. The Pause symbol uses one of the 24 spaces in a dialing sequence.

PBX

See Private Branch Exchange.

Permanent virtual circuit (PVC)

The PVC is an end-to-end virtual connection in frame relay networks.

Peripheral Component Interconnect (PCI) Slot

Socket on the Enterprise Edge Server main board that connect to the Enterprise Edge cards.

Personal Speed Dial

Two-digit codes (71-94) can be programmed to dial external telephone numbers. Personal Speed Dial numbers are programmed for each telephone, and can be used only at the telephone on which they are programmed.

Pickup Group

A telephone can be placed into one of nine call pickup groups. A call ringing at a telephone within a pickup group can be picked up at any other telephone within the same pickup group. A telephone is assigned to a pickup group under Capabilities in Terminals and Sets programming.

Pin-1

The first pin in a multiple-pin connector or chip designated as such to help you properly orient the component when attaching or installing it.

Point-to-point protocol (PPP)

PPP is a protocol for communication between two computers using a serial interface, typically a personal computer connects to a server by a phone line. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP can process synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection.

Pool

See Line pool.

Port

A connector on the Enterprise Edge Server that allows data exchange with other devices, such as a printer or mouse.

portable telephone

See Companion portable telephone

PPP

See Point-to-Point protocol.

Pre-dial

A feature that allows you to enter a number and check it on your telephone display before it is actually dialed. If the number is incorrect, you can edit it. The number is dialed only when you pick up the receiver or select a line.

Primary Rate Interface (PRI)

An ISDN interface which uses twenty three B channels and a D channel (23B+D).

Prime line

The line on your telephone that is automatically selected when you lift the receiver, press the Handsfree/Mute button or use an external dialing feature. A Prime Line is assigned to a telephone under Line access in Terminals and Sets programming.

Prime Set (prime telephone)

A telephone that provides backup answering for incoming calls on external lines. The prime telephone for a line will ring for any unanswered calls on that line. A prime telephone is assigned to a line under Trunk/Line data in Lines programming.

Priority Call

If you get a busy signal when you call someone in your office, you can interrupt them for an urgent call. This feature is enabled for a telephone under Capabilities in Terminals and Sets programming.

Privacy

This feature determines whether a system user may select a line in use at another telephone and join an established call. Privacy is enabled under Trunk/Line data in Lines programming, but can be turned on and off by users during individual calls.

Private branch exchange (PBX)

A PBX is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office.

The PBX is owned and operated by the enterprise rather than the telephone company.

Private line

See Private to.

Private network

A telephone network consisting of owned or leased telephone lines used to connect different offices of an organization independently of the public network.

Private to

Lets you select the telephone that will use the line exclusively. The line cannot appear on any other telephone, except the prime telephone for that line. Private lines cannot be placed into line pools. Private lines are assigned under Trunk/Line data in Lines programming.

programming

Setting the way the Enterprise Edge system will work. Programming includes system-wide settings and individual telephone and line settings.

Protocol

A set of rules and procedures for exchanging data between computers or Enterprise Edge Servers on a network or through the Internet.

Proxy

A proxy is a server that acts on behalf of another.

Power cable

A cable that connects the Enterprise Edge Server to a power source.

public line

An external line that can be assigned to any telephone and to many telephones. A line is assigned as Public under Trunk/Line data in Lines programming.

public network

The regular telephone network that connects most homes and businesses.

pulse/tone dialing

An external line setting for pulse or tone dialing. Pulse is the traditional method of dialing used by rotary-dial or push-button single-line telephones. Tone dialing allows telephones to communicate with other devices such as answering machines. Tone dialing is required to access the features that PBX systems may offer or to use another system remotely.

PVC

See permanent virtual circuit.

Q

Quality of Service (QoS)

On the Internet and in other networks, QoS is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high-bandwidth video and multimedia information.

Using the Internet's Resource Reservation Protocol (RSVP), packets passing through a gateway host can be expedited based on policy and reservation criteria arranged in advance. Using ATM, which also lets a company or user preselect a level of quality in terms of service, QoS can be measured and guaranteed in terms of the average delay at a gateway, the variation in delay in a group of cells (cells are 53-byte transmission units), cell losses, and the transmission error rate.

In Enterprise Edge, QoS is provided over IP. QoS is guaranteed for outgoing traffic until it reaches the next hop.

QoS

See Quality of Service.

R

RAM (Random Access Memory)

Computer memory that stores data temporarily. RAM stores the data used by the microprocessor as it executes instructions. The contents of RAM are erased each time the Enterprise Edge Server is turned off or restarted.

recall

See Link time.

receiver

The handset of a telephone.

Regression Code

Restores the previous system security number so that previously applied UTAM Activation Codes and Portable Credit Codes can be reentered to restore full system operation. Also required in cases of system recovery. This code cannot be reused.

Relaying

Relaying is the process of moving data along a path determined by a routing process. The data is relayed between a source and a destination.

Remind delay

A feature that causes a telephone to beep and display the message `On hold: LINENAM` when a call has been on hold for a programmable period of time. This period is the Remind delay.

Remote access

The ability to dial into an Enterprise Edge system from outside the system and make use of selected features. The lines, features, and dialing capabilities available to a remote user are determined by the Class of Service.

remote access dial restriction

See Remote restriction.

Remote access service(RAS)

The RAS is the ability to get access to a computer or a network from a remote distance. In corporations, people at branch offices, telecommuters, and people who are travelling may need access to the corporation's network. Home users get access to the Internet through remote access to an Internet service provider (ISP).

A remote access server is the computer and associated software that is set up to handle users seeking access to network remotely. Sometimes called a communication server, a remote access server usually includes or is associated with a firewall server to ensure security and a router that can forward the remote access request to another part of the corporate network.

Remote capability

A subset of Enterprise Edge features that are available to users connected through remote access.

Remote device

A remote device is any network device that is accessible only by means of communication over a digital or analog (dial-up) network.

Remote monitoring

A feature that lets an off-site technician with a PC call in and troubleshoot your system through the built-in modem.

Remote paging

This feature allows remote users to use the system paging feature. Access to this feature is governed by the Class of Service for the call. See Remote Access and Class of Service.

Remote restriction

A restriction filter applied to a line in order to control which digits can be dialed during an incoming remote access call. It is the equivalent of a set filter for a remote user.

remote user

Someone who calls into an Enterprise Edge system from a telephone outside that system and uses system features or lines. See Remote Access.

Restriction filter

Through a combination of restrictions and overrides, restriction filters prevent certain telephone numbers or feature codes from being dialed. Restriction filters can be applied to lines, sets, specific lines on a set, and to Class of Service passwords.

Restriction service

A Services section that allows you to assign alternate dialing filters to lines, telephones, lines on a particular telephone, and alternate remote filters to lines at specified times of the day and on specified days.

restrictions

One component of a Dialing filter. Restrictions are numbers you cannot dial when that dialing filter is in effect. See Exceptions.

Ring Again

A feature that can be used when you cannot get through to someone on your system because their telephone is busy or there is no answer. Ring Again instructs the system to inform you when they hang up or next use their telephone.

ring group

A setting under Services that lets you assign a number of different telephones to ring during one of the schedules. Up to 20 ring groups can be programmed by an installer or a system coordinator plus.

ring type

A feature that allows you to select one of four distinctive rings for your telephone.

ring volume

A feature that allows you to set the volume at which your telephone rings.

ringing service

A Services section that allows you to make additional telephones ring at specified times of the day and on specified days.

RIP

See Routing Information Protocol.

Rls button

Ends a call in the same way that hanging up the receiver does.

ROM (Read Only Memory)

Memory that stores data permanently. ROM contains instructions that the Enterprise Edge Server needs to operate. The instructions stored in ROM cannot be changed and are used by the Enterprise Edge Server each time it is turned on or restarted.

Router

A router is a device that forwards traffic between networks, based on network layer information and routing tables. A router decides which path network traffic follows using routing protocols to gain information about the network and algorithms to choose the best route based on a routing matrix.

Routing

The path a message takes from its point of origin to its destination on a network or the Internet.

Routing Information Protocol (RIP)

RIP enables routers in the same autonomous system to exchange routing information by means of periodic updates. RIP is a widely-used protocol for managing routing information within a self-contained network such as a corporate local area network (LAN) or an interconnected group of such LANs.

Using RIP, a gateway host (with a router) sends its entire routing table (which lists all the other hosts is has on record) to its closest neighbor host every 30 seconds. The neighbor host passes the information to its next neighbor and so on until all hosts within the network have the same routing path information, a state known as network convergence. RIP uses a hop count as a way to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet to for a specified destination.

RIP is considered an effective solution for small homogeneous networks. For larger, more complicated networks, RIP's transmission of the entire routing table every 30 seconds may put a heavy amount of extra traffic in the network.

The major alternative to RIP is the Open Shortest Path First Protocol (OSPF).

Routing service

A programming section that allows outgoing calls to be directed automatically based on the numbers a caller dials. For Enterprise Edge Servers linked in a network, routing can create a transparent or coordinated dialing plan. It can also be used to direct calls to the least expensive lines according to a Services schedule (sometimes called least cost routing).

Run / Stop

A feature that creates a break point in a programmed external dialing sequence. When you press a programmed key, the system dials the number up to the run/stop. When you press it again, the system dials the digits following the run/stop.

S

SAPS

See station auxiliary power supply.

Saved Number Redial

A feature that allows you to save the number of the external call you are on (providing you dialed the call) so that you can call it again later.

Schedules

Any of six different sets of services that can be applied to your system. See Services.

Selective line redirection

See Line Redirection.

Serial port

A port that sends and receives data one bit at a time. This port can be used to connect the Enterprise Edge Server to a printer, external modem or mouse. Serial port connector has nine pins and are designated by software with the letters COM and a single digit, such as COM1.

Service modes

See Services.

Services

A programming section that lets you assign which telephones ring, which restrictions apply, and which call routing is used during any of six different schedules. There are three services: Ringing service, Restriction service and Routing service, all found in Services programming.

set

A telephone.

Set Copy

A programming section that allows you to copy programmable settings from one telephone to another of the same type. Set Copy provides two options: duplicating System Data and User Data, or duplicating System Data only. Set Copy does not provide the same copy capability as COPY, which is more selective of the settings that can be duplicated.

Set filter

See Restriction filter.

Set lock (telephone lock)

This feature allows you to limit the number of features that may be used at a telephone. Full set lock allows very few changes or features, Partial set lock allows some changes and features, and No set lock allows any change to be made and any feature to be used. Set lock is assigned under Capabilities in Terminals and Sets programming.

Set relocation

See Automatic Telephone Relocation.

SIMM

Single In-line Memory Module. The Enterprise Edge Server is equipped with one SIMM that provides 64 MB of SDRAM. The memory can be increased with the addition of more SIMMs.

Simple Network Management Protocol (SNMP)

SNMP is the protocol governing network management and the monitoring of network devices and their functions.

SNMP

See Simple Network Management Protocol.

Software keys

A programming section used to enable the optional Remote monitoring feature. One setting provides a System ID, which an installer or system coordinator plus then uses to request three password keys from the Nortel Networks Customer Response Center. Once these three passwords have been entered, the system will permit Remote monitoring.

Startup programming

When an Enterprise Edge system is first installed and powered up, Startup programming must be performed before any programming can be done. Startup initializes the system programming to defaults.

Station

An individual telephone.

Station Auxiliary Power Supply (SAPS)

A device which provides power to a telephone that is connected more than 300 m (975 ft.) and less than 1200 m (3900 ft.) from the server, or to a CAP module.

Station Media Bay Module

A computer module which provides access to telephone lines. The 16-port Digital Station Media Bay Module (EE-DSM 16) allows the connection of 16 digital telephone sets to the system. The 32-port Digital Station Media Bay Module (EE-DSM 32) allows the connection of 32 digital telephone sets to the system. The Analog Station Media Bay Module (EE-ASM 8) allows the connection of analog station sets to the system.

Station set test

A series of diagnostic tests for these components of a telephone: display, buttons, handset, speaker, and power.

subnet mask

A value used to route packets on TCP/IP networks. When the IP layer has to deliver a packet through an interface, it uses the destination address contained in the packet, together with the subnet mask of the interface to select an interface, and the next hop in that subnet

synchronous

A synchronous signal is sourced from the same timing reference. A synchronous signal causes the interval between successive bits, characters, or events to remain constant or locked in to a specific clock frequency.

system data

An option in the Set Copy function. System Data refers to the programmable system settings that apply to all telephones and lines.

System programming

A programming section that lets you assign and maintain certain settings on the Enterprise Edge system.

System speed dial code

A two-digit code (01 to 70) that can be programmed to dial a telephone number up to 24 digits long. System speed dial codes are programmed for the entire system under the System Speed programming heading.

System Startup

See Startup programming.

T

T1

Digital carrier system or line that carries data at 1.544 Mbps.

TAPI

SeeTelephony Application Program Interface.

Target lines

Lines used to answer incoming calls only. A target line routes a call according to digits it receives from an incoming trunk. They are referred to by line numbers in the same way as physical lines.

TCP/IP

See Transmission Control Protocol/Internet Protocol.

TE

See Terminal equipment.

TEI

See Terminal Endpoint Identifier.

Telco features

A programming section that lets you specify the external telephone numbers that are dialed by the Message feature to retrieve voice messages, or to set up CLASS (CMS) services for lines and telephone. Telco features are accessed by an installer or a system coordinator plus.

Telephony Application Program Interface (TAPI)

The Telephony Application Program Interface (TAPI) is a standard program interface that lets you and your computer communicate over telephones or video phones to people or phone-connected resources elsewhere in the world.

Telnet

Telnet is a service that provides terminal-emulation capabilities for logging into the Enterprise Edge unit from a remote location.

Terminal Endpoint Identifier

A digit used to identify devices which are using an ISDN connection for D-channel packet service.

Terminal equipment (TE)

A generic term for devices that connect to an ISDN network. Examples of ISDN TE are ISDN telephones, computers equipped with ISDN cards and video terminals.

Terminals and Sets

A programming section that lets you assign and change settings that apply to the telephones and other devices connected to the Enterprise Edge Server. Terminals and Sets programming is performed by an installer or a system coordinator.

Time and date

A programming section that lets you manually change time or date.

Token-Ring

A token-ring is a network topology and data signaling scheme where a special data packet (called a token) is passed from one station to another along an electrical ring. A transmitting station takes possession of the token, transmits the data, then frees the token after the data has made a complete circuit of the electrical ring.

Tone dial telephone

A push button telephone that emits DTMF tones.

TOS

See Type of Service.

Transfer

A feature that lets you redirect a call to another telephone in your Enterprise Edge system, over a network or outside your system.

Transfer Callback

If a transferred call is not answered after a specific number of rings, the call will return to the telephone that made the transfer. The number of rings is assigned under Feature settings in System programming. Transfer Callback does not apply to calls transferred externally.

Transmission Control Protocol/Internet Protocol (TCP/IP)

A language governing communication among all computers on the Internet.

TCP protocol checks packets of information for errors, submits requests for re-transmission in the event of errors and returns multiple packets of a message into the proper original sequence when the message reaches its destination.

IP dictates how packets are sent out over networks and has a packet addressing method that lets any computer on the Internet forward a packet to any other computer that is a step or more closer to the packet's recipient.

Trunk

The physical connection between the Enterprise Edge system and the outside world using either the public telephone system or a private network.

Trunk Answer

A feature you can use to answer a call on any line that has an active Ringing service Service Mode, even if that line does not appear on your telephone. Trunk Answer is enabled in Services programming.

Trunk Media Bay Module

A computer module which provides access to telecommunications trunks. The Digital Trunk Media Bay Module (EE-DTM) provides the connection between a standard digital PSTN T1 or PRI line and the Enterprise Edge system. The Caller ID Trunk Media Bay Module (EE-CTM) provides the ability to access four analog Caller ID PSTN lines.

Type of Service (TOS)

The TOS field is located in the IP packet header and is used in DiffServ processing.

U

UDP

See User Datagram Protocol.

Unsupervised line

A line for which disconnect supervision is disabled. If an external caller hangs up, the system does not detect the disconnection and does not hang up its line. See Disconnect Supervision.

User Data

User Data is an option in the Set Copy feature. User Data refers to the personal settings that are unique to an individual telephone, and are not programmed for the system. User Data is programmed at each telephone.

These settings, for example, include Personal Speed Dial and the assignment of programmable memory buttons.

User Datagram Protocol (UDP)

The UDP is a protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses IP. UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP.

Like the Transmission Control Protocol, UDP uses IP to actually transfer a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order.

Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

User Filter

See Restriction filter.

User Preferences

A programming section that lets you assign autodialers, user speed dial codes, display contrast, and other settings to a specific telephone or person. You do not have to program these settings at the person's telephone. User preferences are assigned in Terminals and Sets programming.

User Speed Dial

Two-digit codes (71-94) can be programmed to dial external telephone numbers. User Speed Dial numbers are programmed for each telephone, and can be used only at the telephone on which they are programmed.

V

Voice Call

A feature you can use to make an announcement or begin a conversation through the speaker of another telephone in the system. The telephone you call will not ring. Instead, the person you call will hear a beep and then your voice. Their telephone will beep periodically to remind them that their microphone is open.

Voice Call deny

A feature that prevents your telephone from receiving Voice Calls.

Voice message center

If you have subscribed to Call Display services you can receive visual Voice Message Waiting Indication, providing your telephone has a display. If you have Voice Message Waiting Indication, you can program the telephone numbers required to access up to five different Voice Message Centers. You can also program which of the five Centers is to be accessed by each specific line.

Voice over IP (VoIP)

Voice over IP (VoIP) is the capability to deliver voice using the Internet Protocol. VoIP is a set of facilities for managing the delivery of voice information using the IP. In general, this means sending voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public switched telephone network (PSTN). A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service.

In addition to IP, VoIP uses the real-time protocol (RTP) to help ensure that packets get delivered in a timely way. Using public networks, it is difficult to guarantee Quality of Service (QoS).

Using VoIP, an enterprise positions a VoIP device at a gateway. The gateway receives packetized voice transmissions from users within the company and then routes them to other parts of its intranet (local area or wide area network) or, using a T-1 or E-1 interface, sends them over the public switched telephone network.

W

Wait for dial tone

A feature that causes of sequence of numbers to pause until dial tone is present on the line before continuing to dial. The Wait for dial tone symbol (,) uses two of the 24 spaces in a dialing sequence. This feature requires a Services or Combo Cartridge.

Web cache

A web cache is a server or collection of servers that store copies of Internet content. The web cache server can be either located on the LAN where the clients it serves are also located, or it can be embedded within the enterprise WAN or at the client's Internet Service Provider (ISP).

Web proxy

A web proxy, or HTTP proxy, is a server that acts on behalf of the requester of pages from an HTTP server and the Internet.

Weighted Fair Queuing (WFQ)

WFQ is a queuing method that allows low volume traffic such as Telnet to be given priority and interactive traffic receives higher priority than batch transfers. Also, high bandwidth usage traffic such as batch file transfer traffic gets equal priority with other high bandwidth use traffic.

Wide Area Network (WAN)

A collection of computers or Enterprise Edge Servers connected or networked to each other over long distances, typically using common carrier facilities.

wireless

See Companion.

Index

Numerics

2-way DID
PRI 344
PRI dialing plan example 338
2-way service 338

A

access codes 143, 315
accessing Unified Manager settings
resources 63
services 185
system 57
administration
web based, setting up 55
admission control
guidelines 45
introduction 44
alarm
codes 261
CSU 276
messages 138
short term 277
telephone 138
alarm manager settings
overview 231
alarm service settings
overview 226
Alarm time 156
allocating log space 142
allow last number redial
programming 91
ANI (auto number identification) 105
answer
DNs 85
mode 103
with DISA 103
archiving backup files 237
assign
answer DNs 85
intercom buttons 82
line pools 84
lines 83
prime line 82
auto DN, programming 145
auto number identification (see ANI)
Automatic Daylight Savings Time (see Daylight Savings Time)
automatic route selection (see routing)
automatic telephone relocation
programming 280
Automatic Time and Date 138
auxiliary ringer
programming 104
troubleshooting 292

B

background music 137
troubleshooting 293
Backup and Restore
backing up programming 238
caution when restoring programming 239
failed restore 239
file storage 237
starting 238, 239
bar graph (progress indicator) 238
B-channel Sequence 179

C

Call by Call
example 319
PRI limits 154
programming service selection 154
routing
incoming calls 180
routing table 116
service selection for PRI 151
usage metrics 279
call log
automatic 93
password 132
space 94, 142
call log set 93
called ID 93
camp timeout delay 137
CAP (Central Answering Position)
line assignment 84
programming 143
card edge loopback test 273
carrier access codes 124
carrier failure
alarms 275
standard 182
CbC routing table example 116
central answering position (see CAP)
channel
disabling PRI 272
Channel Service Unit (see CSU)

CLASS assignment 93
Class of Service
dialing restriction 308
security 308
Class of Service (see COS)
Clock Source 179
clock source
description 179
primary reference 179
secondary reference 180
timing master 180
CO fail 182
cold start
definition 239
warning (dialog box) 240
common settings 126
Companion
troubleshooting 302
Companion programming
Call Pickup 171
cell
assignment 169
neighbours 169
radio neighbour 170
radios 169
disabling registration 166
enabling registration 166
Group Pickup 171
recommended settings 170
re-evaluation 168
re-evaluation status 168
configuring management settings
alarm manager
overview 231
user manager
overview 229
configuring resource settings
introduction 63
LAN 64
WAN backup links
access parameters 76
link parameters 74
overview 73
summary parameters 74
WAN primary links
access parameters 67
frame relay parameters 70
line parameters 68
overview 66
performance graphs and tables 73
PPP parameters 73
configuring service settings
alarm service
overview 226
DHCP
LAN 187
overview 186
DNS
overview 192
introduction 185
NetLink manager
overview 217
QoS
filters 209
overview 206
performance graphs and tables 209
port ranges 211
QoS monitor
mean opinion score 216
overview 215
routing
LAN 193
overview 192
WAN 201
SNMP
community list 203
manager list 203
overview 202
trap community list 203
Tapi service provider
overview 223
voice mail
overview 227
voice record
access/suppress settings 223
market parameters 221
overview 218
prefix settings 222
report options 220
voice service 224
VoIP Gateway 212
overview 212
Web cache
overview 216
configuring system settings
date 61
fault alarm banner 284
identification 61
introduction 57
name 58
performance graphs and tables 283
resource services 59
time 61
connecting to Enterprise Edge, methods for
remote dial-in 52
connections
stand alone 344
Contrast Adjustment 284

control telephone, programming 126
coordinated dialing plan 310
copy
  telephone settings 80
COS (Class of Service)
  auto DN 145
  calls answered with DISA 145
  password 130
    auto-answer system 306
    line restriction 131
    remote access package 131
    user filter 131
    with DISA 310
CSU (Channel Service Unit)
  alarms 276
  description 183
  line build 182
  performance statistics 276
  stats 274
customizing
  call display services 93

D

date, system 61
Daylight Savings Time, automatic 138
defaults
  dialing restriction 109
  directory number lengths 148
  remote access packages 147
  restrictions 109
  set restrictions 91
delay
  camp timeout 137
  Delayed Ring Transfer 137
  dial signal type 105
  held line reminder 137
  park timeout 137
  transfer callback 137
delayed ring transfer 137
  to prime telephone 137, 139
deprovisioning a line 271
destination code
  description 115, 117
device
  disabling 256
  enabling 257
DHCP
  configuring automatically 38
  guidelines 38
  introduction 37
DHCP service settings
  LAN 187
  overview 186
diagnostics 241
  T1 signal 274
  test results, system test log 257
dial
  mode 102
  tone
    absent on external lines 286
dialed number identification 105
dialing
  restriction
    for remote callers 106
    line filter 131
    line/set restriction 92
    remote user 107
    user filter 131
Dialing Plan
  PRI 344
Dialing plan
  PRI routing table 117
  private DN length 125
  public DN length 124
dialing plan
  2-way DID 338
  coordinated 310
  shared line pools 315
  using T1 E&M lines 312
dialing restriction 308
  defaults 109
  exceptions 110
  maximum length 110
  maximum number 110
  remote 309
  removing a filter 110
  Restriction service 308
  restrictions 110
  set restrictions 91
  wild card character 109, 118
DID (Direct Inward Dial)
  trunk 307
DiffServ networks
  introduction 43
  packet marking 45
Digit Absorb 119
Digit Absorption 119
Digital Trunk Interface (see DTI)
direct-dial digit
  programming 141, 142
direct-dial digit, programming 144
directed pickup 138, 139
directory numbers
  changing 136
  changing starting DN 136
  coordinated dialing plan 310

in a network 310
length 148
DISA (Direct Inward System Access)
DID
trunk 307
DN 145
private networks 331
remote callers 310
disabling
a device 256
a module 254
disconnect
supervision 103
loop start trunks 306
timer 178
disconnect timer 178
display unreadable, troubleshooting 284
DNIS number 105
DNS
gateway 39
guidelines 39
introduction 39
proxy 39
DNS service settings
overview 192
download system settings 241
DSX1 build out 182
DTI (Digital Trunk Interface)
clock source 179
trunk 304
dynamic IP addressing 35

E

EE-DTM
LEDs 294
electromagnetic compatibility 15
enabling
module 255
Enbloc dialing 124
Enterprise Edge
administration, web-based, setting up 55
admission control 44
as a DHCP server 38
IP addresses, setting up
with a laptop 54
with a PC 54
IP routing
information protocol 36
specifics 35
static 36
LAN connections
overview 49
logging off 57
logging on 56
operational considerations 55
packet marking 45
rebooting 57
WAN connections
backup 51
overview 49
permanent 50
frame relay 50
PPP 50
with Meridian M1 over PRI 304
Enterprise Edge Link
programming 89
troubleshooting 291
Enterprise Edge Link settings 89
Enterprise Edge system networking 303
error messages
10.5.2 247
11.12.10 248
11.19.9 247
11.5.2 247
14.17.40 248
14.17.41 248
14.17.68 248
14.4.21 248
14.5.77 248
2.5.4 244
2.5.6 245
2.5.8 245
2.xx.4 245
2.xx.6 245
5.16.68 246
5.4.59 245
5.5.39 245
5.5.40 245
5.5.41 246
5.5.45 246
8.4.2. 246
8.5.3 246
8.8.3 246
9.4.2 247
9.6.4 247
9.6.5 247
9.6.6 247
overview 244
user actions 244
Ethernet
LAN connections 49
WAN connections
backup 51
overview 49
permanent 50
frame relay 50
PPP 50

evening schedule 127
event messages
maintenance 261
significant 262
system restarts 264
exception (see dialing restriction)
extended superframe 182
external
lines
access code 144
paging
troubleshooting 292
external code
programming 144
extra-dial telephone
programming 113

F

fast path routing 37
fault alarm banner settings 284
feature
codes, troubleshooting 299
using remotely 306
files
backup 237
filtering
criteria 350
ranges 350
filters
QoS 209
QoS, adding 210
QoS, deleting 210
QoS, modifying 209
filters (see also restriction service) 92, 108
first display 93
Fnvram (backup file name) 237
frame relay 50
frame relay parameters, WAN 70
framing 182
framing format 182
full autohold 104

G

gateway, DNS 39
ground start trunk 305

H

hardware
clock source 179
modules 178
hearing-aid compatibility 15
held line reminder
remind delay 137
help, customer support 283
hold
tones, music, or silence 137
Hospitality services 155
hung lines 286
Hunt Groups
about 159
Adding members 160
Assigning lines 162
Broadcast mode 163
Distribution modes 163
Moving members 161
Programming busy line setting 164
Programming the overflow set 164
Programming the queue time-out 164
Removing members 160
Rotary mode 163
Sequential mode 163
Setting the hunt delay 163
Setting the name 165
Unassigning lines 162
Hunt groups
usage metrics 279

I

I/F levels 182
ICMP counters 249
identification, system 61
idle line
search for 102
immediate signal type 105
impedance, setting for line 104
incoming call routing
call-by-call 180
Integrated Services Digital Network (see ISDN)
interdigit timeout 125
interface levels 182
internal
numbers
changing 136
length 148
internal CSU 183
internal numbers
coordinated dialing plan 310
in a network 310
IP addresses, setting up
with a laptop 54
with a PC 54
IP addressing
dynamic 35
overview 35
static 35
IP routing

information protocol 36
introduction 34
overview 34
specifics 35
IP services
DHCP
configuring 38
ISDN (Integrated Services Digital Network)
bearer capability 341
capabilities 339
installation programming 345
layers 340
planning service order 340
programming sequence 346
standards 345
ISDN PRI
2-way DID 344
Dialing Plan 344

J

JAVA Virtual Machine (JVM) 55

L

LAN connections 49
LAN resource settings 64
LAN routing services 193
LAN to LAN fast path routing 37
LAN, DHCP settings 187
LEDs
EE-DTM 294
Legacy networks
introduction 43
port range settings 47
line
access 81
assignment 83
deprovisioning 271
filter, programming 131
pool
access code 146
access codes 315
troubleshooting 300
PRI, about 305
programming
name 106
telco features 106
trunk/line data 96
trunk/line data/received number 102
provisioning 271
redirection feature 336
restriction
programming 106
selection, for a direct-dial telephone 143
troubleshooting 285–290
type 101
line coding 182
line parameters, WAN 68
line pool
access code 146
in a dialing plan 310
line restriction 308
line/set restriction 92, 308
user filter 131
link parameters, WAN 74
link time 138, 140
log
network evt 260
space
number of spaces 94
programming 94
space allocation 142
system administration 259
system test 257
logging off of Enterprise Edge 57
logging on to Enterprise Edge 56
logon definitions
configure 57
download 57
login 57
password 57
upload 57
loop start trunk
remote access from public network 306
loopback test
starting 273
loss package 104
loss/gain settings 104
lunch schedule 127

M

M7100 telephone
accessing external lines 144
M7324 telephone
CAP 143
maintenance
alarm codes 261
bipolar violations 277
carrier failure alarms 277
CSU stats 274
disabling module/cartridges 254
enabling the module 255
event messages 261
identify device connected to system 255
module 254
network event log 260
programming
system administration log 258

provisioning 271
short term alarms 277
system
administration log 258
test log 257
version 253
mean opinion score, QoS monitor 216
Meridian 1 316
Message
sending 141
MIB-II
counters 249
variables 249
module
enabling 255
showing inventory 254
troubleshooting 302
moving telephones (see automatic telephone relocation)
music
license 16
source 16

N

name, system 58
National ISDN standards 345
NetLink manager settings
overview 217
network
configuration samples 330–337
coordinated dialing plan 310
event log 260
options with Enterprise Edge 303
private 333
private systems to Enterprise Edge 304
public network to Enterprise Edge 303
security 308
troubleshooting 296–301, 302
user problems 296
Network Name Display 149
Business name 150
calling party name 149
connected name 150
interactions 150
programming 150
receiving redirected name 150
night schedule 127
No free lines 290
Nortel Networks Technical Solutions Centers 283
Not available 290
Not in service 290
NT1 (network termination type 1)
stand alone connections 344

O

on hold (see hold)
open switch interval
disconnect timer 178
operational considerations 55
optional equipment
troubleshooting 291–293
outbound traffic filter, creating 349
Outgoing Name and Number Blocking 172
Outgoing name and number blocking 151
overflow routing 123

P

packet filtering
features
destination address 37
destination mask 37
destination port 37
ICMP code 37
ICMP type 37
protocol 37
source address 37
source mask 37
source port 37
introduction 36
packet marking
DiffServe networks 45
TOS, premium traffic 45
TOS, priority filters 45
Page timeout 140
parameters
obtaining required values 53
required values 53
park
retrieving calls 144
timeout delay 137
park prefix 144
password
calls answered with DISA 145
COS 130
registration 132
using DISA 310
payload loopback test 273
performance 243
performance graphs and tables
QoS 209
system 283
WAN 73
Point to Point Protocol (PPP) 50
port range settings
Legacy networks, overview 47
port ranges
QoS 211

QoS, adding 211
QoS, deleting 212
QoS, modifying 211
service settings 211
portable telephone
disabling 166
enabling 166
troubleshooting 302
PPP parameters, WAN 73
PRI (Primary Rate Interface)
trunk 305
PRI channel
disabling 272
PRI dialing plan
2-way DID 338
PRI line
provisioning 271
PRI line pools 155
PRI Networking
additional configuration 319
Call-by-call services example 319
Meridian 1 316
Meridian M1 configuration 319
prime line 82
prime set 102
prime telephone 137, 139
private line 101
private network 303
remote access 307
sample configurations 333–337
tie lines 331
programming
alarm telephone 138
allow last number redial 91
auto DN 145
backing up 238
CAP assignment 143
features on a set 89, 93, 114
hardware 175
ISDN 346
least cost routing 122
line access 81
lines 95–107
maintenance 233–278
on lines
dialing restrictions 114
ISDN (PRI) lines 346
trunk/line data programming 96
voice message center 107
passwords 130–132
routing 114
services 108–127
software keys 173
system 135–149
system features
auxiliary ringer 114
called ID 93
CLASS assignment 93
DN length 148
extra-dial telephone 113
log space 94
remote restrictions 106
restriction service 91–92, 108, 114
ringing 112
ringing group 113
schedule times 126
services 126
System Speed Dial 128
telco features 91, 106
trunk answer 112, 113
voice message center 107
system speed dial 128
telco features 172
Terminals&Sets 80, 80–94
Programming PRI routing table 117
protocols
routing information 36
provisioning, T1 lines 271
proxy
DNS 39
web caching 40
public line 101
public network 303, 331–332

Q

QoS best effort queue counters 252
QoS best effort traffic counters 251
QoS dropped packets counter 251
QoS filters
adding 210
deleting 210
modifying 209
QoS graph counters 252
QoS module
relationship with the VoIP QoS monitor, overview 48
restrictions and defaults 48
QoS monitor settings
mean opinion score 216
overview 215
QoS port ranges
adding 211
deleting 212
modifying 211
QoS service settings 206
filter 209
performance graphs and tables 209

port ranges 211
QoS session counters 251
Quality of Service (QoS)
overview 42

R

radio-frequency interference 14, 17
reallocating log space 142
rebooting Enterprise Edge 57
received number 102
received number length 148
receiver volume 137
re-evaluation, see Companion programming
registration
information for telephone company 15
on a portable 170
registration password 132
Release Reasons 154
remote
access
COS password 130
defaults 147
from public network 306
loop start trunks 306
programming 131
restricting 146
T1 E&M trunks 306
filters 131
system access 306–307
users, troubleshooting 296–301
remote access
dialing restriction 308
DID trunks 307
on a private network 307
PRI trunk 307
security 308
remote dial-in
guidelines 52
remote restriction 309
remote routers, setting up 349
remote system access 306
resource services settings 59
resource settings, configuring 63
restricting
feature use (see Set Lock)
line at telephone 92
lines 106
remote access 146
remote callers 106
telephones 91, 108
restriction
default 92
dialing 123
service 91, 106, 108
line/set 91, 92
programming 114
schedules 91
restriction service 114
Restrictions
using 308–310
retrieving
voice messages 172
ringing service
night schedule 112
ring group assignment 112
ringing groups 112
RIP, enabling on network interfaces 36
Route
adding a long distance access code 121
dialing plan to route outgoing PRI calls 123
dialing restrictions 123
for least cost routing 122
for local calling 119
for long distance calling 120
routing
destination codes 115
dialing restrictions 123
LAN settings 193
programming 114
sample for local calling 119
sample for long distance calling 120
settings 192
WAN settings 201
routing and IPservices 33
routing, IP
information protocol 36
introduction 34
IP addressing overview 35
managing information 36
overview 34
packet filtering
introduction 36
RIP protocol 36
static 36
routing, LAN to LAN fast path 37

S

sample rate 244
saving settings 241
schedule
names 126
Schedule 4 127
Schedule 5 127
Schedule 6 127
security 308
Class of Service 308

dialing restriction 308
services
evening 127
example of alternate call ringing 112
lunch 127
night 127
programming
common settings 126
restriction services 114
ringing groups 112
ringing service 112
routing service 114
programming ringing sets 113
Schedule 4 127
Schedule 5 127
Schedule 6 127
schedule names 126
schedule times 126
types 111
services, configuring 185
services, IP
DHCP
configuring 38
set
feature and number restrictions 91
restriction
default 91
user filter 131
setting up
JAVA Virtual Machine 55
logging off of Enterprise Edge 57
logging on to Enterprise Edge 56
operational considerations 55
rebooting Enterprise Edge 57
web-based administration 55
settings, saving 241
signal
type 105
significant event messages 262
SNMP
guidelines 41
overview 41
SNMP service settings
community list 203
manager list 203
overview 202
trap community list 203
software keys 173
Speed Dial
programming 128
speed dial 128
start and stop times, services 126
start DN 136
Static DID 338
static IP addressing 35
static IP routing 36
Station Set Test 284
statistics
charts 243
generating 243
sample rate 244
tables 244
Stop restore (dialog box) description 240
summary parameters, WAN 74
superframe 182
support 283
system
administration log 258
processor software 253
sample configurations 330–337
speed dial 128
test log 257, 261, 264
version 253
system performance graphs and tables 283
system programming
change DNS 136
feature settings 136
access codes 143
call log space 142
CAP assignment 143
daylight time 138
Delayed Ring Transfer 139
directd pickup 139
direct-dial 142
held reminder 137
page 138
page tone 138
park 139
set relocation 140
remote access 146
system programming (see system programming)
system settings
Answer key 141
Automatic Time and Date 138
system settings, configuring 57

T

T1
line coding 182
signal diagnostics 274
transmission performance 274
Tapi service provider
overview 223
target lines
and received number 102
description 304

incoming calls 305
numbering 305
TCP counters 251
technical support 283
telephone
control sets 126
direct-dial 144
log calls automatically 93
relocation 140
troubleshooting 284
voice message waiting indication 93
Terminals&Sets 80, 80–94
capabilities 86
allow redirect 87
auxiliary ringer 87
direct-dial 86
DND on busy 86
handsfree 86
handsfree answerback 86
hotline 87
page zone 86
paging 86
pickup group 86
priority call 87
redirect ring 87
line access 81
answer DNs 85
intercom keys 82
line assignment 83
line pool access 84
prime line 82
name 89
restrictions 91
telco features 91
user preferences 90
testing
loopback tests 272
system test log 257
tie lines 331
time, system 61
timer
disconnect 178
TOS
premium traffic 45
priority filters 45
transfer callback 137
troubleshooting 281
auxiliary ringer 292
background music 293
Enterprise Edge Link 291
external paging 292
line pools 300
lines 285
modules 293–295
network or remote users 296–301, 302
optional equipment 291–293
portable telephone 302
T1 signal 295
trunk module 295
trunk modules 293
types of problems 282
trunk
answer, programming 113
DTI 304
ground start 305
mode 103
module
troubleshooting 293, 295
numbering 304
PRI 305
types 304
trunk/line data 96

U

UDP counters 250
unsupervised trunk mode 103
Usage metrics
Call by Call 279
Hunt groups 279
user manager settings
overview 229
utilities
overview 241
performance 243

V

voice mail settings
overview 227
voice message
accessing 93
external center 172
waiting indication 93
voice record
access/suppress settings 223
market parameters settings 221
prefix settings 222
report options settings 220
service settings 218
voice service settings 224
VOIP 100
VoIP gateway settings
local gateway 212
overview 212
remote gateway 212
VoIP QoS Monitor
relationship with the QoS module, overview 48

W

WAN bandwidth, for admission control 44
WAN connections
  backup 51
  overview 49
  permanent 50
    frame relay 50
    PPP 50
WAN resource settings
  backup links
    access parameters 76
    link parameters 74
    overview 73
    summary parameters 74
  primary links
    access parameters 67
    frame relay parameters 70
    line parameters 68
    overview 66
    performance graphs and tables 73
    PPP parameters 73
WAN routing services 201
warm start
  definition 239
Web cache settings
  overview 216
web caching/proxy
  guidelines 40
  introduction 40
web-based administration, setting up 55
wild card character 109, 118
WinkStart signal type 105
wiring
  loopback test 272